

# Computer Networking

# Contents

## Articles

<b>Networking</b>	<b>1</b>
Computer networking	1
Computer network	15
Local area network	29
Campus area network	32
Metropolitan area network	33
Wide area network	34
Wi-Fi Hotspot	36
<b>OSI Model</b>	<b>40</b>
OSI model	40
Physical Layer	48
Media Access Control	51
Logical Link Control	53
Data Link Layer	55
Network Layer	59
Transport Layer	60
Session Layer	64
Presentation Layer	65
Application Layer	67
<b>IEEE 802.1</b>	<b>70</b>
IEEE 802.1D	70
Link Layer Discovery Protocol	71
Spanning tree protocol	73
IEEE 802.1p	84
IEEE 802.1Q	85
IEEE 802.1X	89
<b>IEEE 802.3</b>	<b>95</b>
Ethernet	95
Link aggregation	102
Power over Ethernet	109
Gigabit Ethernet	118

10 Gigabit Ethernet	123
100 Gigabit Ethernet	129
<b>Standards</b>	<b>138</b>
IP address	138
Transmission Control Protocol	144
Internet Protocol	161
IPv4	165
IPv4 address exhaustion	175
IPv6	184
Dynamic Host Configuration Protocol	196
Network address translation	208
Simple Network Management Protocol	219
Internet Protocol Suite	226
Internet Control Message Protocol	236
Internet Group Management Protocol	240
Simple Mail Transfer Protocol	243
Internet Message Access Protocol	252
Lightweight Directory Access Protocol	256
<b>Routing</b>	<b>268</b>
Routing	268
Static routing	273
Link-state routing protocol	274
Open Shortest Path First	278
Routing Information Protocol	289
<b>IEEE 802.11</b>	<b>293</b>
IEEE 802.11	293
IEEE 802.11 (legacy mode)	304
IEEE 802.11a-1999	306
IEEE 802.11b-1999	308
IEEE 802.11g-2003	310
IEEE 802.11n-2009	312
<b>Other</b>	<b>321</b>
Twisted pair	321
Optical fiber	327
Optical fiber connector	346

## References

Article Sources and Contributors	357
Image Sources, Licenses and Contributors	368

## Article Licenses

License	371
---------	-----

# Networking

## Computer networking

A **computer network**, or simply a **network**, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information.<sup>[1]</sup> Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. Simply, more than one computer interconnected through a communication medium for information interchange is called a computer network.

Networks may be classified according to a wide variety of characteristics, such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope.

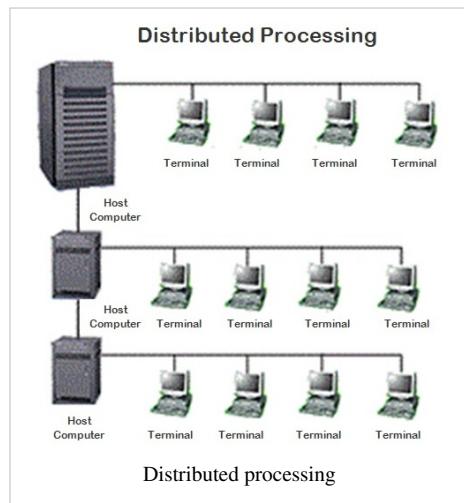
Communications protocols define the rules and data formats for exchanging information in a computer network, and provide the basis for network programming. Well-known communications protocols include Ethernet, a hardware and link layer standard that is ubiquitous in local area networks, and the Internet protocol suite, which defines a set of protocols for internetworking, i.e. for data communication between multiple networks, as well as host-to-host data transfer, and application-specific data transmission formats.

Computer networking is sometimes considered a sub-discipline of electrical engineering, telecommunications, computer science, information technology or computer engineering, since it relies upon the theoretical and practical application of these disciplines.

## History

Before the advent of computer networks that were based upon some type of telecommunications system, communication between calculation machines and early computers was performed by human users by carrying instructions between them. Many of the social behaviors seen in today's Internet were demonstrably present in the 19th century and arguably in even earlier networks using visual signals.

- In September 1940, George Stibitz used a Teletype machine to send instructions for a problem set from his Model at Dartmouth College to his Complex Number Calculator in New York and received results back by the same means. Linking output systems like teletypewriters to computers was an interest at the Advanced Research Projects Agency (ARPA) when, in 1962, J.C.R. Licklider was hired and developed a working group he called the "Intergalactic Computer Network", a precursor to the ARPANET.
- Early networks of communicating computers included the military radar system Semi-Automatic Ground Environment (SAGE), started in the late 1950s.
- The commercial airline reservation system semi-automatic business research environment (SABRE) went online with two connected mainframes in 1960.<sup>[2][3]</sup>
- In 1964, researchers at Dartmouth developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at Massachusetts Institute of Technology, a research group supported by



General Electric and Bell Labs used a computer to route and manage telephone connections.

- Throughout the 1960s Leonard Kleinrock, Paul Baran and Donald Davies independently conceptualized and developed network systems which used packets that could be used in a network between computer systems.
- 1965 Thomas Marill and Lawrence G. Roberts created the first wide area network (WAN). This was an immediate precursor to the ARPANET, of which Roberts became program manager.
- The first widely used telephone switch that used true computer control was introduced by Western Electric in 1965.
- In 1969 the University of California at Los Angeles, the Stanford Research Institute, University of California at Santa Barbara, and the University of Utah were connected as the beginning of the ARPANET network using 50 kbit/s circuits.<sup>[4]</sup>
- Commercial services using X.25 were deployed in 1972, and later used as an underlying infrastructure for expanding TCP/IP networks.

Today, computer networks are the core of modern communication. All modern aspects of the public switched telephone network (PSTN) are computer-controlled, and telephony increasingly runs over the Internet Protocol, although not necessarily the public Internet. The scope of communication has increased significantly in the past decade, and this boom in communications would not have been possible without the progressively advancing computer network. Computer networks, and the technologies needed to connect and communicate through and between them, continue to drive computer hardware, software, and peripherals industries. This expansion is mirrored by growth in the numbers and types of users of networks, from the researcher to the home user.

Interconnected collection of autonomous computers(unique identity) is known as computer network.

## Properties

Computer networks:

Facilitate communications

Using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.

Permit sharing of files, data, and other types of information

In a network environment, authorized users may access data and information stored on other computers on the network. The capability of providing access to data and information on shared storage devices is an important feature of many networks.

May be insecure

A computer network may be used by computer hackers to deploy computer viruses or computer worms on devices connected to the network, or to prevent these devices from normally accessing the network (denial of service).

May interfere with other technologies

Power line communication strongly disturbs certain<sup>[5]</sup> forms of radio communication, e.g., amateur radio.<sup>[6]</sup> It may also interfere with last mile access technologies such as ADSL and VDSL.<sup>[7]</sup>

May be difficult to set up

A complex computer network may be difficult to set up. It may also be very costly to set up an effective computer network in a large organization or company.

---

## Communication media

Computer networks can be classified according to the hardware and associated software technology that is used to interconnect the individual devices in the network, such as electrical cable (HomePNA, power line communication, G.hn), optical fiber, and radio waves (wireless LAN). In the OSI model, these are located at levels 1 and 2.

A well-known *family* of communication media is collectively known as Ethernet. It is defined by IEEE 802 and utilizes various standards and media that enable communication between devices. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium.

### Wired technologies

The order of the following wired technologies is, roughly, from slowest to fastest transmission speed.

- *Twisted pair wire* is the most widely used medium for telecommunication. Twisted-pair cabling consists of copper wires that are twisted into pairs. Ordinary telephone wires consist of two insulated copper wires twisted into pairs. Computer networking cabling (wired Ethernet as defined by IEEE 802.3) consists of 4 pairs of copper cabling that can be utilized for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2 million bits per second to 10 billion bits per second. Twisted pair cabling comes in two forms: unshielded twisted pair (UTP) and shielded twisted-pair (STP). Each form comes in several category ratings, designed for use in various scenarios.
- *Coaxial cable* is widely used for cable television systems, office buildings, and other work-sites for local area networks. The cables consist of copper or aluminum wire surrounded by an insulating layer (typically a flexible material with a high dielectric constant), which itself is surrounded by a conductive layer. The insulation helps minimize interference and distortion. Transmission speed ranges from 200 million bits per second to more than 500 million bits per second.
- ITU-T G.hn technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed (up to 1 Gigabit/s) local area network.
- An optical fiber is a glass fiber. It uses pulses of light to transmit data. Some advantages of optical fibers over metal wires are less transmission loss, immunity from electromagnetic radiation, and very fast transmission speed, up to trillions of bits per second. One can use different colors of lights to increase the number of messages being sent over a fiber optic cable.

### Wireless technologies

- *Terrestrial microwave* – Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low-gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km (**unknown operator: u'strong' mi**) apart.
- *Communications satellites* – The satellites communicate via microwave radio waves, which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically in geosynchronous orbit **unknown operator: u','unknown operator: u','unknown operator: u','(unknown operator: u'strong'unknown operator: u','mi)** above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.
- *Cellular and PCS systems* use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.
- *Radio and spread spectrum technologies* – Wireless local area network use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology

to enable communication between multiple devices in a limited area. IEEE 802.11 defines a common flavor of open-standards wireless radio-wave technology.

- Infrared communication can transmit signals for small distances, typically no more than 10 meters. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices.
- A global area network (GAN) is a network used for supporting mobile across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial wireless LANs.<sup>[8]</sup>

## Exotic technologies

There have been various attempts at transporting data over more or less exotic media:

- IP over Avian Carriers was a humorous April fool's Request for Comments, issued as **RFC 1149**. It was implemented in real life in 2001.<sup>[9]</sup>
- Extending the Internet to interplanetary dimensions via radio waves.<sup>[10]</sup>

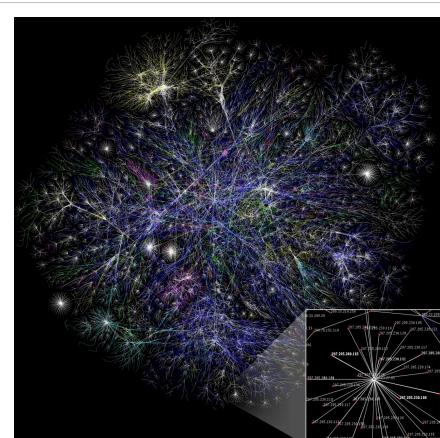
Both cases have a large round-trip delay time, which prevents useful communication.

## Communications protocols and network programming

A communications protocol is a set of rules for exchanging information over a network. It is typically a protocol stack (also see the OSI model), which is a "stack" of protocols, in which each protocol uses the protocol below it. An important example of a protocol stack is HTTP running over TCP over IP over IEEE 802.11 (TCP and IP are members of the Internet Protocol Suite, and IEEE 802.11 is a member of the Ethernet protocol suite). This stack is used between the wireless router and the home user's personal computer when the user is surfing the web.

Communication protocols have various properties, such as whether they are connection-oriented or connectionless, whether they use circuit mode or packet switching, or whether they use hierarchical or flat addressing.

There are many communication protocols, a few of which are described below.



Internet map. The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide.

## Ethernet

Ethernet is a family of protocols used in LANs, described by a set of standards together called IEEE 802 published by the Institute of Electrical and Electronics Engineers. It has a flat addressing scheme and is mostly situated at levels 1 and 2 of the OSI model. For home users today, the most well-known member of this protocol family is IEEE 802.11, otherwise known as Wireless LAN (WLAN). However, the complete protocol suite deals with a multitude of networking aspects not only for home use, but especially when the technology is deployed to support a diverse range of business needs. MAC bridging (IEEE 802.1D) deals with the routing of Ethernet packets using a Spanning Tree Protocol, IEEE 802.1Q describes VLANs, and IEEE 802.1X defines a port-based Network Access Control protocol, which forms the basis for the authentication mechanisms used in VLANs, but it is also found in WLANs – it is what the home user sees when the user has to enter a "wireless access key".

## Internet Protocol Suite

The Internet Protocol Suite, often also called TCP/IP, is the foundation of all modern internetworking. It offers connection-less as well as connection-oriented services over an inherently unreliable network traversed by datagram transmission at the Internet protocol (IP) level. At its core, the protocol suite defines the addressing, identification, and routing specification in form of the traditional Internet Protocol Version 4 (IPv4) and IPv6, the next generation of the protocol with a much enlarged addressing capability.

## SONET/SDH

Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers. They were originally designed to transport circuit mode communications from a variety of different sources, primarily to support real-time, uncompressed, circuit-switched voice encoded in PCM(Pulse-Code Modulation) format. However, due to its protocol neutrality and transport-oriented features, SONET/SDH also was the obvious choice for transporting Asynchronous Transfer Mode (ATM) frames.

## Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells. This differs from other protocols such as the Internet Protocol Suite or Ethernet that use variable sized packets or frames. ATM has similarity with both circuit and packet switched networking. This makes it a good choice for a network that must handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.

While the role of ATM is diminishing in favor of next-generation networks, it still plays a role in the last mile, which is the connection between an Internet service provider and the home user. For an interesting write-up of the technologies involved, including the deep stacking of communications protocols used, see.<sup>[11]</sup>

## Network programming

Computer network programming involves writing computer programs that communicate with each other across a computer network. Different programs must be written for the client process, which initiates the communication, and for the server process, which waits for the communication to be initiated. Both endpoints of the communication flow are implemented as network sockets; hence network programming is basically socket programming.

## Scale

Networks are often classified by their physical or organizational extent or their purpose. Usage, trust level, and access rights differ between these types of networks.

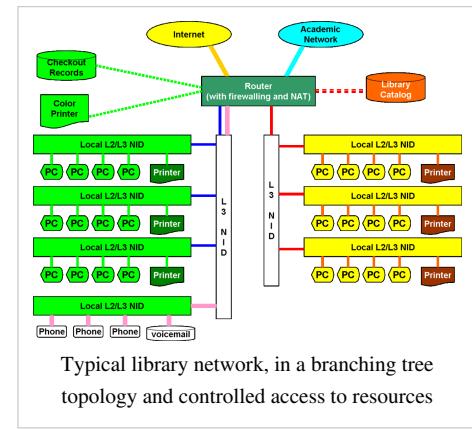
## Personal area network

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters.<sup>[12]</sup> A wired PAN is usually constructed with USB and Firewire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

## Local area network

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T G.hn also provide a way to create a wired LAN using existing home wires (coaxial cables, phone lines and power lines).<sup>[13]</sup>

A sample LAN is depicted in the accompanying diagram. All interconnected devices must understand the network layer (layer 3), because they are handling multiple subnets (the different colors). Those inside the library, which have only 10/100 Mbit/s Ethernet connections to the user device and a Gigabit Ethernet connection to the central router, could be called "layer 3 switches" because they only have Ethernet interfaces and must understand IP. It would be more correct to call them access routers, where the router at the top is a distribution router that connects to the Internet and academic networks' customer access routers.



The defining characteristics of LANs, in contrast to WANs (Wide Area Networks), include their higher data transfer rates, smaller geographic range, and no need for leased telecommunication lines. Current Ethernet or other IEEE 802.3 LAN technologies operate at data transfer rates up to 10 Gbit/s. IEEE has projects investigating the standardization of 40 and 100 Gbit/s.<sup>[14]</sup> LANs can be connected to Wide area network by using routers.

## Home area network

A home area network (HAN) is a residential LAN which is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable TV or Digital Subscriber Line (DSL) provider.

## Storage area network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The cost and complexity of SANs dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium sized business environments.

## Campus area network

A campus area network (CAN) is a computer network made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc.) are almost entirely owned (by the campus tenant / owner: an enterprise, university, government etc.).

In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including, for example, academic colleges or departments, the university library, and student residence halls.

## Backbone network

A backbone network is part of a computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than that of the networks connected to it.

A large corporation which has many locations may have a backbone network that ties all of these locations together, for example, if a server cluster needs to be accessed by different departments of a company which are located at different geographical locations. The equipment which ties these departments together constitute the network backbone. Network performance management including network congestion are critical parameters taken into account when designing a network backbone.

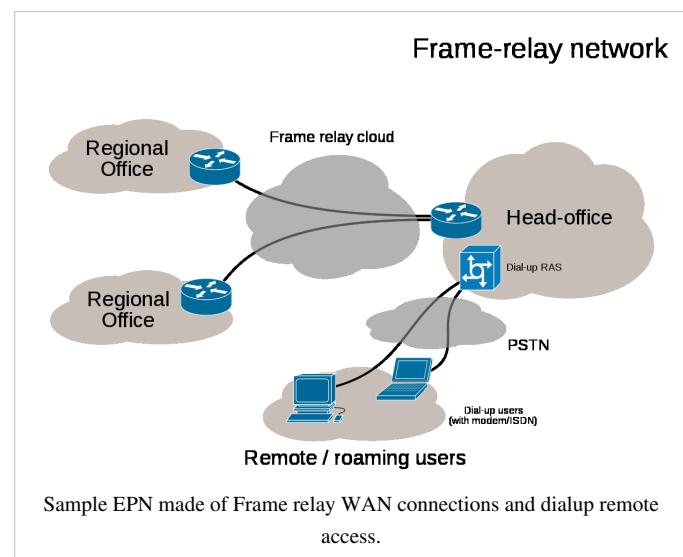
A specific case of a backbone network is the Internet backbone, which is the set of wide-area network connections and core routers that interconnect all networks connected to the Internet.

## Metropolitan area network

A Metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.

## Wide area network

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

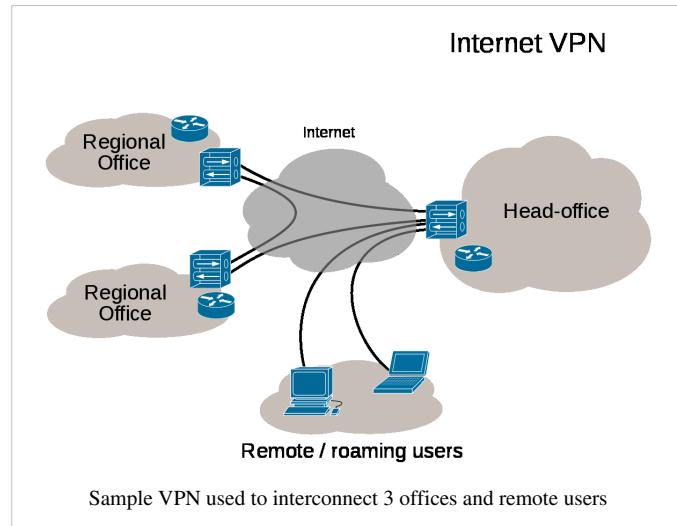


## Enterprise private network

An enterprise private network is a network built by an enterprise to interconnect various company sites, e.g., production sites, head offices, remote offices, shops, in order to share computer resources.

## Virtual private network

A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.



VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

## Virtual Network

Not to be confused with a Virtual Private Network, a Virtual Network defines data traffic flows between virtual machines within a hypervisor in a virtual computing environment. Virtual Networks may employ virtual security switches, virtual routers, virtual firewalls and other virtual networking devices to direct and secure data traffic.

## Internetwork

An internetwork is the connection of multiple computer networks via a common routing technology using routers. The Internet is an aggregation of many connected internetworks spanning the Earth.

## Organizational scope

Networks are typically managed by organizations which own them. According to the owner's point of view, networks are seen as intranets or extranets. A special case of network is the Internet, which has no single owner but a distinct status when seen by an organizational entity – that of permitting virtually unlimited global connectivity for a great multitude of purposes.

## Intranets and extranets

Intranets and extranets are parts or extensions of a computer network, usually a LAN.

An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer applications, that is under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

An extranet is a network that is limited in scope to a single organization or entity and also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities—a company's customers may be given access to some part of its intranet—while at the same time the customers may not be considered *trusted* from a security standpoint. Technically, an extranet may also be categorized as a CAN, MAN,

WAN, or other type of network, although an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

## Internet

The Internet is a global system of interconnected governmental, academic, corporate, public, and private computer networks. It is based on the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the United States Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW).

Participants in the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet Protocol Suite and an addressing system (IP addresses) administered by the Internet Assigned Numbers Authority and address registries. Service providers and large enterprises exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

## Network topology

### Common layouts

A network topology is the layout of the interconnections of the nodes of a computer network. Common layouts are:

- A bus network: all nodes are connected to a common medium along this medium. This was the layout used in the original Ethernet, called 10BASE5 and 10BASE2.
- A star network: all nodes are connected to a special central node. This is the typical layout found in a Wireless LAN, where each wireless client connects to the central Wireless access point.
- A ring network: each node is connected to its left and right neighbour node, such that all nodes are connected and that each node can reach each other node by traversing nodes left- or rightwards. The Fiber Distributed Data Interface (FDDI) made use of such a topology.
- A mesh network: each node is connected to an arbitrary number of neighbours in such a way that there is at least one traversal from any node to any other.
- A fully connected network: each node is connected to every other node in the network.

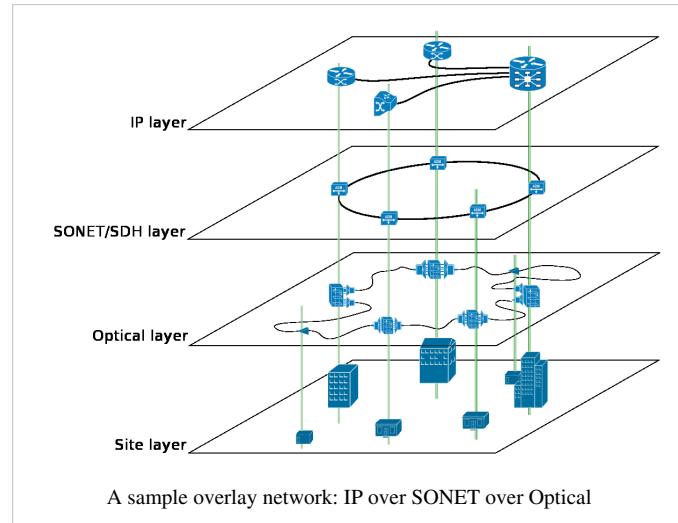
Note that the physical layout of the nodes in a network may not necessarily reflect the network topology. As an example, with FDDI, the network topology is a ring (actually two counter-rotating rings), but the physical topology is a star, because all neighboring connections are routed via a central physical location.

## Overlay network

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay are connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one.

For example, many peer-to-peer networks are overlay networks because they are organized as nodes of a virtual system of links run on top of the Internet. The Internet was initially built as an overlay on the telephone network.<sup>[15]</sup>

The most striking example of an overlay network, however, is the Internet itself: At the IP layer, each node can reach any other by a direct connection to the desired IP address, thereby creating a fully connected network; the underlying network, however, is composed of a mesh-like interconnect of subnetworks of varying topologies (and, in fact, technologies). Address resolution and routing are the means which allows the mapping of the fully connected IP overlay network to the underlying ones.



Overlay networks have been around since the invention of networking when computer systems were connected over telephone lines using modems, before any data network existed.

Another example of an overlay network is a distributed hash table, which maps keys to nodes in the network. In this case, the underlying network is an IP network, and the overlay network is a table (actually a map) indexed by keys.

Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. Previous proposals such as IntServ, DiffServ, and IP Multicast have not seen wide acceptance largely because they require modification of all routers in the network. On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes a message traverses before reaching its destination.

For example, Akamai Technologies manages an overlay network that provides reliable, efficient content delivery (a kind of multicast). Academic research includes end system multicast<sup>[16]</sup> and overcast for multicast; RON (resilient overlay network) for resilient routing; and OverQoS for quality of service guarantees, among others.

## Basic hardware components

Apart from the physical communications media themselves as described above, networks comprise additional basic hardware building blocks interconnecting their terminals, such as network interface cards (NICs), hubs, bridges, switches, and routers.

### Network interface cards

A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to physically access a networking medium. It provides a low-level addressing system through the use of MAC addresses.

Each Ethernet network interface has a unique MAC address which is usually stored in a small memory device on the card, allowing any device to connect to the network without creating an address conflict. Ethernet MAC addresses are composed of six octets. Uniqueness is maintained by the IEEE, which manages the Ethernet address space by assigning 3-octet prefixes to equipment manufacturers. The list of prefixes<sup>[17]</sup> is publicly available. Each manufacturer is then obliged to both use only their assigned prefix(es) and to uniquely set the 3-octet suffix of every Ethernet interface they produce.

## Repeaters and hubs

A repeater is an electronic device that receives a signal, cleans it of unnecessary noise, regenerates it, and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. A repeater with multiple ports is known as a hub. Repeaters work on the Physical Layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row (e.g. Ethernet's 5-4-3 rule).

Today, repeaters and hubs have been made mostly obsolete by switches (see below).

## Bridges

A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges broadcast to all ports except the port on which the broadcast was received. However, bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address to that port only.

Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Bridges come in three basic types:

- Local bridges: Directly connect LANs
- Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.
- Wireless bridges: Can be used to join LANs or connect remote stations to LANs.

## Switches

A network switch is a device that forwards and filters OSI layer 2 datagrams (chunks of data communication) between ports (connected cables) based on the MAC addresses in the packets.<sup>[18]</sup> A switch is distinct from a hub in that it only forwards the frames to the ports involved in the communication rather than all ports connected. A switch breaks the collision domain but represents itself as a broadcast domain. Switches make forwarding decisions of frames on the basis of MAC addresses. A switch normally has numerous ports, facilitating a star topology for devices, and cascading additional switches.<sup>[19]</sup> Some switches are capable of routing based on Layer 3 addressing or additional logical levels; these are called multi-layer switches. The term *switch* is used loosely in marketing to encompass devices including routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier).

## Routers

A router is an internetworking device that forwards packets between networks by processing information found in the datagram or packet (Internet protocol information from Layer 3 of the OSI Model). In many situations, this information is processed in conjunction with the routing table (also known as forwarding table). Routers use routing tables to determine what interface to forward packets (this can include the "null" also known as the "black hole" interface because data can go into it, however, no further processing is done for said data).

## Firewalls

A firewall is an important aspect of a network with respect to security. It typically rejects access requests from unsafe sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in 'cyber' attacks for the purpose of stealing/corrupting data, planting viruses, etc.

## Network performance

**Network performance** refers to the service quality of a telecommunications product as seen by the customer. It should not be seen merely as an attempt to get "more through" the network.

The following list gives examples of Network Performance measures for a circuit-switched network and one type of packet-switched network, viz. ATM:

- Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads.<sup>[20]</sup> Other types of performance measures can include noise, echo and so on.
- ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.<sup>[21]</sup>

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modelled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.<sup>[22]</sup>

## Network security

In the field of networking, the area of **network security**<sup>[23]</sup> consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network security is the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network Security covers a variety of computer networks, both public and private that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

## Network resilience

In computer networking: “**Resilience** is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.”<sup>[24]</sup>

## Views of networks

Users and network administrators typically have different views of their networks. Users can share printers and some servers from a workgroup, which usually means they are in the same geographic location and are on the same LAN, whereas a Network Administrator is responsible to keep that network up and running. A community of interest has less of a connection of being in a local area, and should be thought of as a set of arbitrarily located users who share a set of servers, and possibly also communicate via peer-to-peer technologies.

Network administrators can see networks from both physical and logical perspectives. The physical perspective involves geographic locations, physical cabling, and the network elements (e.g., routers, bridges and application layer gateways) that interconnect the physical media. Logical networks, called, in the TCP/IP architecture, subnets, map onto one or more physical media. For example, a common practice in a campus of buildings is to make a set of LAN cables in each building appear to be a common subnet, using virtual LAN (VLAN) technology.

Both users and administrators will be aware, to varying extents, of the trust and scope characteristics of a network. Again using TCP/IP architectural terminology, an intranet is a community of interest under private administration usually by an enterprise, and is only accessible by authorized users (e.g. employees).<sup>[25]</sup> Intranets do not have to be connected to the Internet, but generally have a limited connection. An extranet is an extension of an intranet that allows secure communications to users outside of the intranet (e.g. business partners, customers).<sup>[25]</sup>

Unofficially, the Internet is the set of users, enterprises, and content providers that are interconnected by Internet Service Providers (ISP). From an engineering viewpoint, the Internet is the set of subnets, and aggregates of subnets, which share the registered IP address space and exchange information about the reachability of those IP addresses using the Border Gateway Protocol. Typically, the human-readable names of servers are translated to IP addresses, transparently to users, via the directory function of the Domain Name System (DNS).

Over the Internet, there can be business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) communications. Especially when money or sensitive information is exchanged, the communications are apt to be **secured** by some form of communications security mechanism. Intranets and extranets can be securely superimposed onto the Internet, without any access by general Internet users and administrators, using secure Virtual Private Network (VPN) technology.

## References

- [1] Computer network definition (<http://www.atis.org/glossary/definition.aspx?id=6555>), , retrieved 2011-11-12
- [2] Michael A. Banks (2008). *On the way to the web: the secret history of the internet and its founders* (<http://books.google.com/books?id=P9wbSjO9WMMC&pg=PA1>). Apress. p. 1. ISBN 978-1-4302-0869-3. .
- [3] Christos J. P. Moschovitis (1998). *History of the Internet: a chronology, 1843 to the present* ([http://books.google.com/?id=Hu5SAAAAMAAJ&dq=intitle:"history+of+the+internet"+sage+sabre&q=sage+sabre's#search\\_anchor](http://books.google.com/?id=Hu5SAAAAMAAJ&dq=intitle:"history+of+the+internet"+sage+sabre&q=sage+sabre's#search_anchor)). ABC-CLIO. p. 36. ISBN 978-1-57607-118-2. .
- [4] Chris Sutton. "Internet Began 35 Years Ago at UCLA with First Message Ever Sent Between Two Computers" (<http://web.archive.org/web/20080308120314/http://www.engineer.ucla.edu/stories/2004/Internet35.htm>). *UCLA*. Archived from the original (<http://www.engineer.ucla.edu/stories/2004/Internet35.htm>) on March 8, 2008. .
- [5] Andrew S Tanenbaum,4th Edition. Pearson Education/PHI.
- [6] *Broadband Over Powerline* (<http://www.arrl.org/broadband-over-powerline-bpl>), The National Association for Amateur Radio, , retrieved 2011-11-12
- [7] "The Likelihood and Extent of Radio Frequency Interference from In-Home PLT Devices" (<http://stakeholders.ofcom.org.uk/binaries/research/technology-research/pltreport.pdf>). Ofcom. . Retrieved 18 June 2011.
- [8] "Mobile Broadband Wireless connections (MBWA)" (<http://grouper.ieee.org/groups/802/20/>). . Retrieved 2011-11-12.
- [9] Bergen Linux User Group's CPIP Implementation (<http://www.blug.linux.no/rfc1149>)

- [10] A. Hooke (September 2000), *Interplanetary Internet* (<http://www.ipnsig.org/reports/ISART9-2000.pdf>), Third Annual International Symposium on Advanced Radio Technologies, , retrieved 2011-11-12
- [11] Martin, Thomas. "Design Principles for DSL-Based Access Solutions" ([http://www.gsi.dit.upm.es/~legf/Varios/XDSL\\_MARTI.PDF](http://www.gsi.dit.upm.es/~legf/Varios/XDSL_MARTI.PDF)). . Retrieved 18 June 2011.
- [12] "personal area network (PAN)" ([http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40\\_gci546288,00.html](http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci546288,00.html)). . Retrieved January 29, 2011.
- [13] *New global standard for fully networked home* (<http://www.itu.int/ITU-T/newslog/New+Global+Standard+For+Fully+Networked+Home.aspx>), ITU-T, 2008-12-12, , retrieved 2011-11-12
- [14] *IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force* (<http://www.ieee802.org/3/ba/>), , retrieved 2011-11-12
- [15] D. Andersen; H. Balakrishnan; M. Kaashoek; R. Morris (10-2001), *Resilient Overlay Networks* (<http://nms.lcs.mit.edu/papers/ron-sosp2001.html>), Association for Computing Machinery, , retrieved 2011-11-12
- [16] <http://esm.cs.cmu.edu/>
- [17] <http://standards.ieee.org/regauth/oui/oui.txt>
- [18] "Define switch." (<http://www.webopedia.com/TERM/s/switch.html>). WWW.Wikipedia.com. . Retrieved April 8, 2008.
- [19] "Basic Components of a Local Area Network (LAN)" (<http://networkbits.net/lan-components/local-area-network-lan-basic-components/>). NetworkBits.net. . Retrieved April 8, 2008.
- [20] *Teletraffic Engineering Handbook* (<http://web.archive.org/web/20070111015452/http://oldwww.com.dtu.dk/teletraffic/handbook/telenook.pdf>), ITU-T Study Group 2, archived from the original (<http://www.com.dtu.dk/teletraffic/handbook/telenook.pdf>) on 2007-01-11,
- [21] Telecommunications Magazine Online (<http://www.telecommagazine.com>), Americas January 2003, Issue Highlights, Online Exclusive: Broadband Access Maximum Performance, Retrieved on February 13, 2005.
- [22] "State Transition Diagrams" ([http://cne.gmu.edu/modules/os\\_perf/std.t.html](http://cne.gmu.edu/modules/os_perf/std.t.html)). . Retrieved July 13, 2003.
- [23] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". *Lecture Notes in Computer Science*. Lecture Notes in Computer Science **3285**: 317–323. doi:10.1007/978-3-540-30176-9\_41. ISBN 978-3-540-23659-7.
- [24] "Definitions: Resilience" ([http://wiki.ittc.ku.edu/resilinets\\_wiki/index.php/Definitions#Resilience](http://wiki.ittc.ku.edu/resilinets_wiki/index.php/Definitions#Resilience)). ResiliNets Research Initiative. . Retrieved 2011-11-12.
- [25] RFC 2547
- ⌚ This article incorporates public domain material from the General Services Administration document "Federal Standard 1037C" (<http://www.its.blrdoc.gov/fs-1037/fs-1037c.htm>).

## Further reading

- Shelly, Gary, et al. "Discovering Computers" 2003 Edition
- Cisco Systems, Inc., (2003, March 14). CCNA: network media types. Retrieved from ciscopress.com (<http://www.ciscopress.com/articles/article.asp?p=31276&rll=1>)
- Wendell Odom,Rus Healy, Denise Donohue. (2010) CCIE Routing and Switching. Indianapolis, IN: Cisco Press
- Kurose James F and Keith W. Ross : Computer Networking: A Top-Down Approach Featuring the Internet, Pearson Education 2005.
- Andrew S. Tanenbaum, *Computer Networks*, Fourth Edition, Pearson Education 2006 (ISBN 0-13-349945-6).
- William Stallings, *Computer Networking with Internet Protocols and Technology*, Pearson Education 2004.
- Important publications in computer networks
- Vinton G. Cerf "Software: Global Infrastructure for the 21st Century" (<http://www.cs.washington.edu/homes/lazowska/cra/networks.html>)
- Meyers, Mike, "Mike Meyers' Certification Passport: Network+" ISBN 0-07-225348-7"
- Odom, Wendall, "CCNA Certification Guide"
- Network Communication Architecture and Protocols: OSI Network Architecture 7 Layers Model

## External links

- Easy Network Concepts (<http://www.netfilter.org/documentation/HOWTO/networking-concepts-HOWTO.html>) (Linux kernel specific)
- Computer Networks and Protocol ([http://nsgn.net/osi\\_reference\\_model/](http://nsgn.net/osi_reference_model/)) (Research document, 2006)
- Computer Networking Glossary (<http://compnetworking.about.com/od/basicnetworkingconcepts/l/blglossary.htm>)
- Networking (<http://www.dmoz.org/Computers/Software/Networking/>) at the Open Directory Project

# Computer network

A **computer network**, or simply a **network**, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information.<sup>[1]</sup> Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. Simply, more than one computer interconnected through a communication medium for information interchange is called a computer network.

Networks may be classified according to a wide variety of characteristics, such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope.

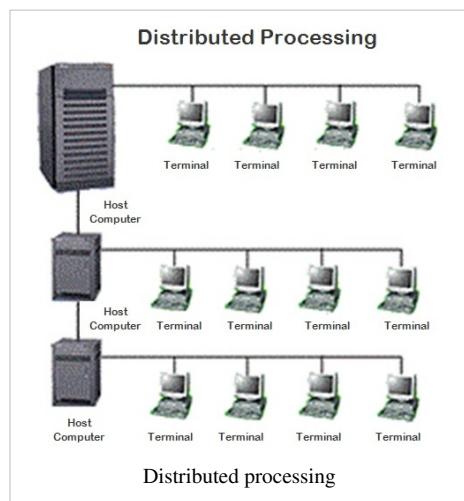
Communications protocols define the rules and data formats for exchanging information in a computer network, and provide the basis for network programming. Well-known communications protocols include Ethernet, a hardware and link layer standard that is ubiquitous in local area networks, and the Internet protocol suite, which defines a set of protocols for internetworking, i.e. for data communication between multiple networks, as well as host-to-host data transfer, and application-specific data transmission formats.

Computer networking is sometimes considered a sub-discipline of electrical engineering, telecommunications, computer science, information technology or computer engineering, since it relies upon the theoretical and practical application of these disciplines.

## History

Before the advent of computer networks that were based upon some type of telecommunications system, communication between calculation machines and early computers was performed by human users by carrying instructions between them. Many of the social behaviors seen in today's Internet were demonstrably present in the 19th century and arguably in even earlier networks using visual signals.

- In September 1940, George Stibitz used a Teletype machine to send instructions for a problem set from his Model at Dartmouth College to his Complex Number Calculator in New York and received results back by the same means. Linking output systems like teletypewriters to computers was an interest at the Advanced Research Projects Agency (ARPA) when, in 1962, J.C.R. Licklider was hired and developed a working group he called the "Intergalactic Computer Network", a precursor to the ARPANET.
- Early networks of communicating computers included the military radar system Semi-Automatic Ground Environment (SAGE), started in the late 1950s.



- The commercial airline reservation system semi-automatic business research environment (SABRE) went online with two connected mainframes in 1960.<sup>[2][3]</sup>
- In 1964, researchers at Dartmouth developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at Massachusetts Institute of Technology, a research group supported by General Electric and Bell Labs used a computer to route and manage telephone connections.
- Throughout the 1960s Leonard Kleinrock, Paul Baran and Donald Davies independently conceptualized and developed network systems which used packets that could be used in a network between computer systems.
- 1965 Thomas Marill and Lawrence G. Roberts created the first wide area network (WAN). This was an immediate precursor to the ARPANET, of which Roberts became program manager.
- The first widely used telephone switch that used true computer control was introduced by Western Electric in 1965.
- In 1969 the University of California at Los Angeles, the Stanford Research Institute, University of California at Santa Barbara, and the University of Utah were connected as the beginning of the ARPANET network using 50 kbit/s circuits.<sup>[4]</sup>
- Commercial services using X.25 were deployed in 1972, and later used as an underlying infrastructure for expanding TCP/IP networks.

Today, computer networks are the core of modern communication. All modern aspects of the public switched telephone network (PSTN) are computer-controlled, and telephony increasingly runs over the Internet Protocol, although not necessarily the public Internet. The scope of communication has increased significantly in the past decade, and this boom in communications would not have been possible without the progressively advancing computer network. Computer networks, and the technologies needed to connect and communicate through and between them, continue to drive computer hardware, software, and peripherals industries. This expansion is mirrored by growth in the numbers and types of users of networks, from the researcher to the home user.

Interconnected collection of autonomous computers(unique identity) is known as computer network.

## Properties

Computer networks:

Facilitate communications

Using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.

Permit sharing of files, data, and other types of information

In a network environment, authorized users may access data and information stored on other computers on the network. The capability of providing access to data and information on shared storage devices is an important feature of many networks.

May be insecure

A computer network may be used by computer hackers to deploy computer viruses or computer worms on devices connected to the network, or to prevent these devices from normally accessing the network (denial of service).

May interfere with other technologies

Power line communication strongly disturbs certain<sup>[5]</sup> forms of radio communication, e.g., amateur radio.<sup>[6]</sup> It may also interfere with last mile access technologies such as ADSL and VDSL.<sup>[7]</sup>

May be difficult to set up

A complex computer network may be difficult to set up. It may also be very costly to set up an effective computer network in a large organization or company.

---

## Communication media

Computer networks can be classified according to the hardware and associated software technology that is used to interconnect the individual devices in the network, such as electrical cable (HomePNA, power line communication, G.hn), optical fiber, and radio waves (wireless LAN). In the OSI model, these are located at levels 1 and 2.

A well-known *family* of communication media is collectively known as Ethernet. It is defined by IEEE 802 and utilizes various standards and media that enable communication between devices. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium.

### Wired technologies

The order of the following wired technologies is, roughly, from slowest to fastest transmission speed.

- *Twisted pair wire* is the most widely used medium for telecommunication. Twisted-pair cabling consists of copper wires that are twisted into pairs. Ordinary telephone wires consist of two insulated copper wires twisted into pairs. Computer networking cabling (wired Ethernet as defined by IEEE 802.3) consists of 4 pairs of copper cabling that can be utilized for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed ranges from 2 million bits per second to 10 billion bits per second. Twisted pair cabling comes in two forms: unshielded twisted pair (UTP) and shielded twisted-pair (STP). Each form comes in several category ratings, designed for use in various scenarios.
- *Coaxial cable* is widely used for cable television systems, office buildings, and other work-sites for local area networks. The cables consist of copper or aluminum wire surrounded by an insulating layer (typically a flexible material with a high dielectric constant), which itself is surrounded by a conductive layer. The insulation helps minimize interference and distortion. Transmission speed ranges from 200 million bits per second to more than 500 million bits per second.
- ITU-T G.hn technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed (up to 1 Gigabit/s) local area network.
- An optical fiber is a glass fiber. It uses pulses of light to transmit data. Some advantages of optical fibers over metal wires are less transmission loss, immunity from electromagnetic radiation, and very fast transmission speed, up to trillions of bits per second. One can use different colors of lights to increase the number of messages being sent over a fiber optic cable.

### Wireless technologies

- *Terrestrial microwave* – Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low-gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km (**unknown operator: u'strong' mi**) apart.
- *Communications satellites* – The satellites communicate via microwave radio waves, which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically in geosynchronous orbit **unknown operator: u','unknown operator: u','unknown operator: u','(unknown operator: u'strong'unknown operator: u','mi)** above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.
- *Cellular and PCS systems* use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.
- *Radio and spread spectrum technologies* – Wireless local area network use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology

to enable communication between multiple devices in a limited area. IEEE 802.11 defines a common flavor of open-standards wireless radio-wave technology.

- Infrared communication can transmit signals for small distances, typically no more than 10 meters. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices.
- A global area network (GAN) is a network used for supporting mobile across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial wireless LANs.<sup>[8]</sup>

## Exotic technologies

There have been various attempts at transporting data over more or less exotic media:

- IP over Avian Carriers was a humorous April fool's Request for Comments, issued as **RFC 1149**. It was implemented in real life in 2001.<sup>[9]</sup>
- Extending the Internet to interplanetary dimensions via radio waves.<sup>[10]</sup>

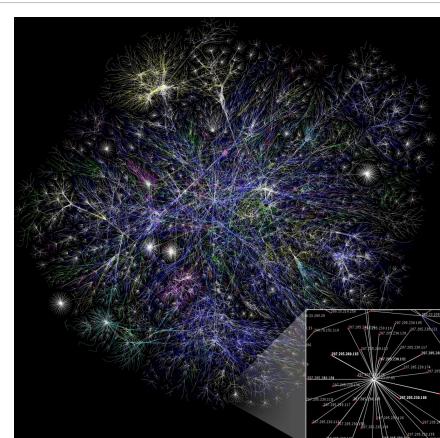
Both cases have a large round-trip delay time, which prevents useful communication.

## Communications protocols and network programming

A communications protocol is a set of rules for exchanging information over a network. It is typically a protocol stack (also see the OSI model), which is a "stack" of protocols, in which each protocol uses the protocol below it. An important example of a protocol stack is HTTP running over TCP over IP over IEEE 802.11 (TCP and IP are members of the Internet Protocol Suite, and IEEE 802.11 is a member of the Ethernet protocol suite). This stack is used between the wireless router and the home user's personal computer when the user is surfing the web.

Communication protocols have various properties, such as whether they are connection-oriented or connectionless, whether they use circuit mode or packet switching, or whether they use hierarchical or flat addressing.

There are many communication protocols, a few of which are described below.



Internet map. The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide.

## Ethernet

Ethernet is a family of protocols used in LANs, described by a set of standards together called IEEE 802 published by the Institute of Electrical and Electronics Engineers. It has a flat addressing scheme and is mostly situated at levels 1 and 2 of the OSI model. For home users today, the most well-known member of this protocol family is IEEE 802.11, otherwise known as Wireless LAN (WLAN). However, the complete protocol suite deals with a multitude of networking aspects not only for home use, but especially when the technology is deployed to support a diverse range of business needs. MAC bridging (IEEE 802.1D) deals with the routing of Ethernet packets using a Spanning Tree Protocol, IEEE 802.1Q describes VLANs, and IEEE 802.1X defines a port-based Network Access Control protocol, which forms the basis for the authentication mechanisms used in VLANs, but it is also found in WLANs – it is what the home user sees when the user has to enter a "wireless access key".

## Internet Protocol Suite

The Internet Protocol Suite, often also called TCP/IP, is the foundation of all modern internetworking. It offers connection-less as well as connection-oriented services over an inherently unreliable network traversed by datagram transmission at the Internet protocol (IP) level. At its core, the protocol suite defines the addressing, identification, and routing specification in form of the traditional Internet Protocol Version 4 (IPv4) and IPv6, the next generation of the protocol with a much enlarged addressing capability.

## SONET/SDH

Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers. They were originally designed to transport circuit mode communications from a variety of different sources, primarily to support real-time, uncompressed, circuit-switched voice encoded in PCM(Pulse-Code Modulation) format. However, due to its protocol neutrality and transport-oriented features, SONET/SDH also was the obvious choice for transporting Asynchronous Transfer Mode (ATM) frames.

## Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells. This differs from other protocols such as the Internet Protocol Suite or Ethernet that use variable sized packets or frames. ATM has similarity with both circuit and packet switched networking. This makes it a good choice for a network that must handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.

While the role of ATM is diminishing in favor of next-generation networks, it still plays a role in the last mile, which is the connection between an Internet service provider and the home user. For an interesting write-up of the technologies involved, including the deep stacking of communications protocols used, see.<sup>[11]</sup>

## Network programming

Computer network programming involves writing computer programs that communicate with each other across a computer network. Different programs must be written for the client process, which initiates the communication, and for the server process, which waits for the communication to be initiated. Both endpoints of the communication flow are implemented as network sockets; hence network programming is basically socket programming.

## Scale

Networks are often classified by their physical or organizational extent or their purpose. Usage, trust level, and access rights differ between these types of networks.

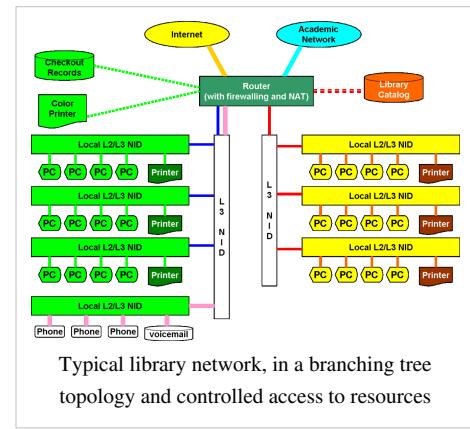
## Personal area network

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters.<sup>[12]</sup> A wired PAN is usually constructed with USB and Firewire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

## Local area network

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T G.hn also provide a way to create a wired LAN using existing home wires (coaxial cables, phone lines and power lines).<sup>[13]</sup>

A sample LAN is depicted in the accompanying diagram. All interconnected devices must understand the network layer (layer 3), because they are handling multiple subnets (the different colors). Those inside the library, which have only 10/100 Mbit/s Ethernet connections to the user device and a Gigabit Ethernet connection to the central router, could be called "layer 3 switches" because they only have Ethernet interfaces and must understand IP. It would be more correct to call them access routers, where the router at the top is a distribution router that connects to the Internet and academic networks' customer access routers.



The defining characteristics of LANs, in contrast to WANs (Wide Area Networks), include their higher data transfer rates, smaller geographic range, and no need for leased telecommunication lines. Current Ethernet or other IEEE 802.3 LAN technologies operate at data transfer rates up to 10 Gbit/s. IEEE has projects investigating the standardization of 40 and 100 Gbit/s.<sup>[14]</sup> LANs can be connected to Wide area network by using routers.

## Home area network

A home area network (HAN) is a residential LAN which is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable TV or Digital Subscriber Line (DSL) provider.

## Storage area network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The cost and complexity of SANs dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium sized business environments.

## Campus area network

A campus area network (CAN) is a computer network made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc.) are almost entirely owned (by the campus tenant / owner: an enterprise, university, government etc.).

In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including, for example, academic colleges or departments, the university library, and student residence halls.

## Backbone network

A backbone network is part of a computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than that of the networks connected to it.

A large corporation which has many locations may have a backbone network that ties all of these locations together, for example, if a server cluster needs to be accessed by different departments of a company which are located at different geographical locations. The equipment which ties these departments together constitute the network backbone. Network performance management including network congestion are critical parameters taken into account when designing a network backbone.

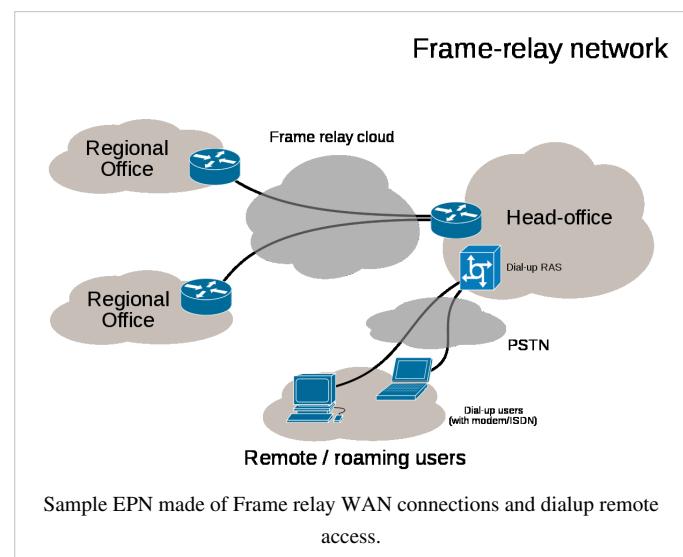
A specific case of a backbone network is the Internet backbone, which is the set of wide-area network connections and core routers that interconnect all networks connected to the Internet.

## Metropolitan area network

A Metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.

## Wide area network

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

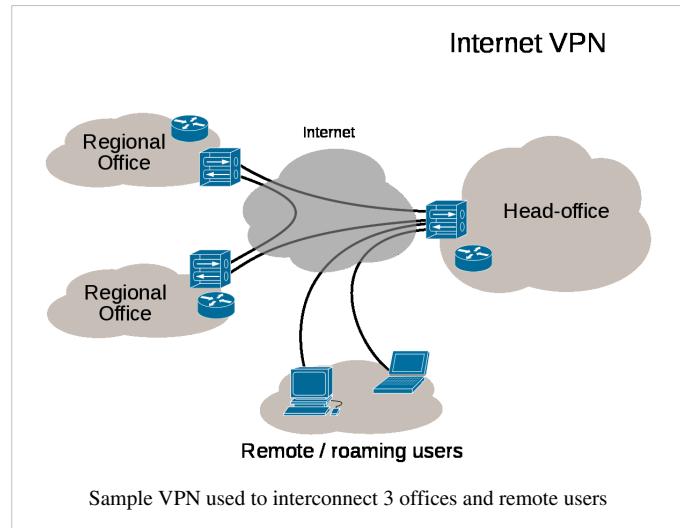


## Enterprise private network

An enterprise private network is a network built by an enterprise to interconnect various company sites, e.g., production sites, head offices, remote offices, shops, in order to share computer resources.

## Virtual private network

A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.



VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

## Virtual Network

Not to be confused with a Virtual Private Network, a Virtual Network defines data traffic flows between virtual machines within a hypervisor in a virtual computing environment. Virtual Networks may employ virtual security switches, virtual routers, virtual firewalls and other virtual networking devices to direct and secure data traffic.

## Internetwork

An internetwork is the connection of multiple computer networks via a common routing technology using routers. The Internet is an aggregation of many connected internetworks spanning the Earth.

## Organizational scope

Networks are typically managed by organizations which own them. According to the owner's point of view, networks are seen as intranets or extranets. A special case of network is the Internet, which has no single owner but a distinct status when seen by an organizational entity – that of permitting virtually unlimited global connectivity for a great multitude of purposes.

## Intranets and extranets

Intranets and extranets are parts or extensions of a computer network, usually a LAN.

An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer applications, that is under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

An extranet is a network that is limited in scope to a single organization or entity and also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities—a company's customers may be given access to some part of its intranet—while at the same time the customers may not be considered *trusted* from a security standpoint. Technically, an extranet may also be categorized as a CAN, MAN,

WAN, or other type of network, although an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

## Internet

The Internet is a global system of interconnected governmental, academic, corporate, public, and private computer networks. It is based on the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the United States Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW).

Participants in the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet Protocol Suite and an addressing system (IP addresses) administered by the Internet Assigned Numbers Authority and address registries. Service providers and large enterprises exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

## Network topology

### Common layouts

A network topology is the layout of the interconnections of the nodes of a computer network. Common layouts are:

- A bus network: all nodes are connected to a common medium along this medium. This was the layout used in the original Ethernet, called 10BASE5 and 10BASE2.
- A star network: all nodes are connected to a special central node. This is the typical layout found in a Wireless LAN, where each wireless client connects to the central Wireless access point.
- A ring network: each node is connected to its left and right neighbour node, such that all nodes are connected and that each node can reach each other node by traversing nodes left- or rightwards. The Fiber Distributed Data Interface (FDDI) made use of such a topology.
- A mesh network: each node is connected to an arbitrary number of neighbours in such a way that there is at least one traversal from any node to any other.
- A fully connected network: each node is connected to every other node in the network.

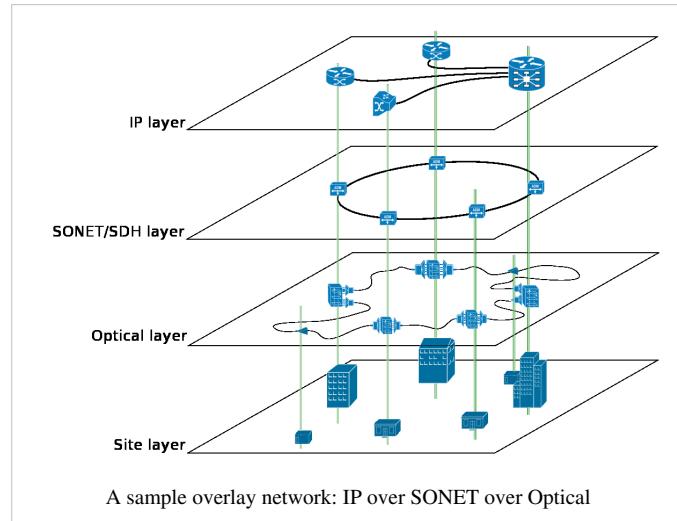
Note that the physical layout of the nodes in a network may not necessarily reflect the network topology. As an example, with FDDI, the network topology is a ring (actually two counter-rotating rings), but the physical topology is a star, because all neighboring connections are routed via a central physical location.

## Overlay network

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay are connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one.

For example, many peer-to-peer networks are overlay networks because they are organized as nodes of a virtual system of links run on top of the Internet. The Internet was initially built as an overlay on the telephone network.<sup>[15]</sup>

The most striking example of an overlay network, however, is the Internet itself: At the IP layer, each node can reach any other by a direct connection to the desired IP address, thereby creating a fully connected network; the underlying network, however, is composed of a mesh-like interconnect of subnetworks of varying topologies (and, in fact, technologies). Address resolution and routing are the means which allows the mapping of the fully connected IP overlay network to the underlying ones.



Overlay networks have been around since the invention of networking when computer systems were connected over telephone lines using modems, before any data network existed.

Another example of an overlay network is a distributed hash table, which maps keys to nodes in the network. In this case, the underlying network is an IP network, and the overlay network is a table (actually a map) indexed by keys.

Overlay networks have also been proposed as a way to improve Internet routing, such as through quality of service guarantees to achieve higher-quality streaming media. Previous proposals such as IntServ, DiffServ, and IP Multicast have not seen wide acceptance largely because they require modification of all routers in the network. On the other hand, an overlay network can be incrementally deployed on end-hosts running the overlay protocol software, without cooperation from Internet service providers. The overlay has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes a message traverses before reaching its destination.

For example, Akamai Technologies manages an overlay network that provides reliable, efficient content delivery (a kind of multicast). Academic research includes end system multicast<sup>[16]</sup> and overcast for multicast; RON (resilient overlay network) for resilient routing; and OverQoS for quality of service guarantees, among others.

## Basic hardware components

Apart from the physical communications media themselves as described above, networks comprise additional basic hardware building blocks interconnecting their terminals, such as network interface cards (NICs), hubs, bridges, switches, and routers.

### Network interface cards

A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to physically access a networking medium. It provides a low-level addressing system through the use of MAC addresses.

Each Ethernet network interface has a unique MAC address which is usually stored in a small memory device on the card, allowing any device to connect to the network without creating an address conflict. Ethernet MAC addresses are composed of six octets. Uniqueness is maintained by the IEEE, which manages the Ethernet address space by assigning 3-octet prefixes to equipment manufacturers. The list of prefixes<sup>[17]</sup> is publicly available. Each manufacturer is then obliged to both use only their assigned prefix(es) and to uniquely set the 3-octet suffix of every Ethernet interface they produce.

## Repeaters and hubs

A repeater is an electronic device that receives a signal, cleans it of unnecessary noise, regenerates it, and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. A repeater with multiple ports is known as a hub. Repeaters work on the Physical Layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row (e.g. Ethernet's 5-4-3 rule).

Today, repeaters and hubs have been made mostly obsolete by switches (see below).

## Bridges

A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges broadcast to all ports except the port on which the broadcast was received. However, bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address to that port only.

Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Bridges come in three basic types:

- Local bridges: Directly connect LANs
- Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.
- Wireless bridges: Can be used to join LANs or connect remote stations to LANs.

## Switches

A network switch is a device that forwards and filters OSI layer 2 datagrams (chunks of data communication) between ports (connected cables) based on the MAC addresses in the packets.<sup>[16]</sup> A switch is distinct from a hub in that it only forwards the frames to the ports involved in the communication rather than all ports connected. A switch breaks the collision domain but represents itself as a broadcast domain. Switches make forwarding decisions of frames on the basis of MAC addresses. A switch normally has numerous ports, facilitating a star topology for devices, and cascading additional switches.<sup>[17]</sup> Some switches are capable of routing based on Layer 3 addressing or additional logical levels; these are called multi-layer switches. The term *switch* is used loosely in marketing to encompass devices including routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier).

## Routers

A router is an internetworking device that forwards packets between networks by processing information found in the datagram or packet (Internet protocol information from Layer 3 of the OSI Model). In many situations, this information is processed in conjunction with the routing table (also known as forwarding table). Routers use routing tables to determine what interface to forward packets (this can include the "null" also known as the "black hole" interface because data can go into it, however, no further processing is done for said data).

## Firewalls

A firewall is an important aspect of a network with respect to security. It typically rejects access requests from unsafe sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in 'cyber' attacks for the purpose of stealing/corrupting data, planting viruses, etc.

## Network performance

**Network performance** refers to the service quality of a telecommunications product as seen by the customer. It should not be seen merely as an attempt to get "more through" the network.

The following list gives examples of Network Performance measures for a circuit-switched network and one type of packet-switched network, viz. ATM:

- Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads.<sup>[18]</sup> Other types of performance measures can include noise, echo and so on.
- ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.<sup>[19]</sup>

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modelled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.<sup>[20]</sup>

## Network security

In the field of networking, the area of **network security**<sup>[21]</sup> consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. Network security is the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network Security covers a variety of computer networks, both public and private that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

## Network resilience

In computer networking: “**Resilience** is the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.”<sup>[22]</sup>

## Views of networks

Users and network administrators typically have different views of their networks. Users can share printers and some servers from a workgroup, which usually means they are in the same geographic location and are on the same LAN, whereas a Network Administrator is responsible to keep that network up and running. A community of interest has less of a connection of being in a local area, and should be thought of as a set of arbitrarily located users who share a set of servers, and possibly also communicate via peer-to-peer technologies.

Network administrators can see networks from both physical and logical perspectives. The physical perspective involves geographic locations, physical cabling, and the network elements (e.g., routers, bridges and application layer gateways) that interconnect the physical media. Logical networks, called, in the TCP/IP architecture, subnets, map onto one or more physical media. For example, a common practice in a campus of buildings is to make a set of LAN cables in each building appear to be a common subnet, using virtual LAN (VLAN) technology.

Both users and administrators will be aware, to varying extents, of the trust and scope characteristics of a network. Again using TCP/IP architectural terminology, an intranet is a community of interest under private administration usually by an enterprise, and is only accessible by authorized users (e.g. employees).<sup>[23]</sup> Intranets do not have to be connected to the Internet, but generally have a limited connection. An extranet is an extension of an intranet that allows secure communications to users outside of the intranet (e.g. business partners, customers).<sup>[23]</sup>

Unofficially, the Internet is the set of users, enterprises, and content providers that are interconnected by Internet Service Providers (ISP). From an engineering viewpoint, the Internet is the set of subnets, and aggregates of subnets, which share the registered IP address space and exchange information about the reachability of those IP addresses using the Border Gateway Protocol. Typically, the human-readable names of servers are translated to IP addresses, transparently to users, via the directory function of the Domain Name System (DNS).

Over the Internet, there can be business-to-business (B2B), business-to-consumer (B2C) and consumer-to-consumer (C2C) communications. Especially when money or sensitive information is exchanged, the communications are apt to be **secured** by some form of communications security mechanism. Intranets and extranets can be securely superimposed onto the Internet, without any access by general Internet users and administrators, using secure Virtual Private Network (VPN) technology.

## References

- [1] Computer network definition (<http://www.atis.org/glossary/definition.aspx?id=6555>), , retrieved 2011-11-12
- [2] Michael A. Banks (2008). *On the way to the web: the secret history of the internet and its founders* (<http://books.google.com/books?id=P9wbSjO9WMMC&pg=PA1>). Apress. p. 1. ISBN 978-1-4302-0869-3. .
- [3] Christos J. P. Moschovitis (1998). *History of the Internet: a chronology, 1843 to the present* ([http://books.google.com/?id=Hu5SAAAAMAAJ&dq=intitle:"history+of+the+internet"+sage+sabre&q=sage+sabre's#search\\_anchor](http://books.google.com/?id=Hu5SAAAAMAAJ&dq=intitle:"history+of+the+internet"+sage+sabre&q=sage+sabre's#search_anchor)). ABC-CLIO. p. 36. ISBN 978-1-57607-118-2. .
- [4] Chris Sutton. "Internet Began 35 Years Ago at UCLA with First Message Ever Sent Between Two Computers" (<http://web.archive.org/web/20080308120314/http://www.engineer.ucla.edu/stories/2004/Internet35.htm>). *UCLA*. Archived from the original (<http://www.engineer.ucla.edu/stories/2004/Internet35.htm>) on March 8, 2008. .
- [5] Andrew S Tanenbaum,4th Edition. Pearson Education/PHI.
- [6] *Broadband Over Powerline* (<http://www.arrl.org/broadband-over-powerline-bpl>), The National Association for Amateur Radio, , retrieved 2011-11-12
- [7] "The Likelihood and Extent of Radio Frequency Interference from In-Home PLT Devices" (<http://stakeholders.ofcom.org.uk/binaries/research/technology-research/pltreport.pdf>). Ofcom. . Retrieved 18 June 2011.
- [8] "Mobile Broadband Wireless connections (MBWA)" (<http://grouper.ieee.org/groups/802/20/>). . Retrieved 2011-11-12.
- [9] Bergen Linux User Group's CPIP Implementation (<http://www.blug.linux.no/rfc1149>)

- [10] A. Hooke (September 2000), *Interplanetary Internet* (<http://www.ipnsig.org/reports/ISART9-2000.pdf>), Third Annual International Symposium on Advanced Radio Technologies, , retrieved 2011-11-12
  - [11] Martin, Thomas. "Design Principles for DSL-Based Access Solutions" ([http://www.gsi.dit.upm.es/~legf/Varios/XDSL\\_MARTI.PDF](http://www.gsi.dit.upm.es/~legf/Varios/XDSL_MARTI.PDF)). . Retrieved 18 June 2011.
  - [12] "personal area network (PAN)" ([http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40\\_gci546288,00.html](http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci546288,00.html)). . Retrieved January 29, 2011.
  - [13] *New global standard for fully networked home* (<http://www.itu.int/ITU-T/newslog/New+Global+Standard+For+Fully+Networked+Home.aspx>), ITU-T, 2008-12-12, , retrieved 2011-11-12
  - [14] *IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force* (<http://www.ieee802.org/3/ba/>), , retrieved 2011-11-12
  - [15] D. Andersen; H. Balakrishnan; M. Kaashoek; R. Morris (10-2001), *Resilient Overlay Networks* (<http://nms.lcs.mit.edu/papers/ron-sosp2001.html>), Association for Computing Machinery, , retrieved 2011-11-12
  - [16] "Define switch." (<http://www.webopedia.com/TERM/s/switch.html>). WWW.Wikipedia.com. . Retrieved April 8, 2008.
  - [17] "Basic Components of a Local Area Network (LAN)" (<http://networkbits.net/lan-components/local-area-network-lan-basic-components/>). NetworkBits.net. . Retrieved April 8, 2008.
  - [18] *Teletraffic Engineering Handbook* (<http://web.archive.org/web/20070111015452/http://oldwww.com.dtu.dk/teletraffic/handbook/telenook.pdf>), ITU-T Study Group 2, archived from the original (<http://www.com.dtu.dk/teletraffic/handbook/telenook.pdf>) on 2007-01-11,
  - [19] Telecommunications Magazine Online (<http://www.telecommagazine.com>), Americas January 2003, Issue Highlights, Online Exclusive: Broadband Access Maximum Performance, Retrieved on February 13, 2005.
  - [20] "State Transition Diagrams" ([http://cne.gmu.edu/modules/os\\_perf/std.t.html](http://cne.gmu.edu/modules/os_perf/std.t.html)). . Retrieved July 13, 2003.
  - [21] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". *Lecture Notes in Computer Science*. Lecture Notes in Computer Science **3285**: 317–323. doi:10.1007/978-3-540-30176-9\_41. ISBN 978-3-540-23659-7.
  - [22] "Definitions: Resilience" ([http://wiki.ittc.ku.edu/resilinets\\_wiki/index.php/Definitions#Resilience](http://wiki.ittc.ku.edu/resilinets_wiki/index.php/Definitions#Resilience)). ResiliNets Research Initiative. . Retrieved 2011-11-12.
  - [23] RFC 2547
- © This article incorporates public domain material from the General Services Administration document "Federal Standard 1037C" (<http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm>).

## Further reading

- Shelly, Gary, et al. "Discovering Computers" 2003 Edition
- Cisco Systems, Inc., (2003, March 14). CCNA: network media types. Retrieved from ciscopress.com (<http://www.ciscopress.com/articles/article.asp?p=31276&rll=1>)
- Wendell Odom,Rus Healy, Denise Donohue. (2010) CCIE Routing and Switching. Indianapolis, IN: Cisco Press
- Kurose James F and Keith W. Ross : Computer Networking: A Top-Down Approach Featuring the Internet, Pearson Education 2005.
- Andrew S. Tanenbaum, *Computer Networks*, Fourth Edition, Pearson Education 2006 (ISBN 0-13-349945-6).
- William Stallings, *Computer Networking with Internet Protocols and Technology*, Pearson Education 2004.
- Important publications in computer networks
- Vinton G. Cerf "Software: Global Infrastructure for the 21st Century" (<http://www.cs.washington.edu/homes/lazowska/cra/networks.html>)
- Meyers, Mike, "Mike Meyers' Certification Passport: Network+" ISBN 0-07-225348-7"
- Odom, Wendall, "CCNA Certification Guide"
- Network Communication Architecture and Protocols: OSI Network Architecture 7 Layers Model

## External links

- Easy Network Concepts (<http://www.netfilter.org/documentation/HOWTO/networking-concepts-HOWTO.html>) (Linux kernel specific)
- Computer Networks and Protocol ([http://nsgn.net/osi\\_reference\\_model/](http://nsgn.net/osi_reference_model/)) (Research document, 2006)
- Computer Networking Glossary (<http://compnetworking.about.com/od/basicnetworkingconcepts/l/blglossary.htm>)
- Networking (<http://www.dmoz.org/Computers/Software/Networking/>) at the Open Directory Project

## Local area network

A **local area network (LAN)** is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building using network media.<sup>[1]</sup> The defining characteristics of LANs, in contrast to wide area networks (WANs), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

ARCNET, Token Ring and other technology standards have been used in the past, but Ethernet over twisted pair cabling, and Wi-Fi are the two most common technologies currently used to build LANs.

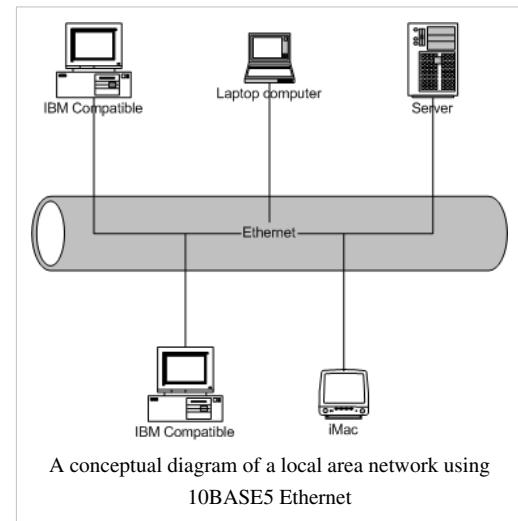
## History

The increasing demand and use of computers in universities and research labs in the late 1960s generated the need to provide high-speed interconnections between computer systems. A 1970 report from the Lawrence Radiation Laboratory detailing the growth of their "Octopus" network<sup>[2][3]</sup> gave a good indication of the situation.

Cambridge Ring was developed at Cambridge University in 1974<sup>[4]</sup> but was never developed into a successful commercial product.

Ethernet was developed at Xerox PARC in 1973–1975,<sup>[5]</sup> and filed as U.S. Patent 4063220<sup>[6]</sup>. In 1976, after the system was deployed at PARC, Metcalfe and Boggs published a seminal paper, "Ethernet: Distributed Packet-Switching For Local Computer Networks."<sup>[7]</sup>

ARCNET was developed by Datapoint Corporation in 1976 and announced in 1977.<sup>[8]</sup> It had the first commercial installation in December 1977 at Chase Manhattan Bank in New York.<sup>[9]</sup>



## Standards evolution

The development and proliferation of personal computers using the CP/M operating system in the late 1970s, and later DOS-based systems starting in 1981, meant that many sites grew to dozens or even hundreds of computers. The initial driving force for networking was generally to share storage and printers, which were both expensive at the time. There was much enthusiasm for the concept and for several years, from about 1983 onward, computer industry pundits would regularly declare the coming year to be "the year of the LAN".<sup>[10][11][12]</sup>

In practice, the concept was marred by proliferation of incompatible physical layer and network protocol implementations, and a plethora of methods of sharing resources. Typically, each vendor would have its own type of

network card, cabling, protocol, and network operating system. A solution appeared with the advent of Novell NetWare which provided even-handed support for dozens of competing card/cable types, and a much more sophisticated operating system than most of its competitors. Netware dominated<sup>[13]</sup> the personal computer LAN business from early after its introduction in 1983 until the mid 1990s when Microsoft introduced Windows NT Advanced Server and Windows for Workgroups.

Of the competitors to NetWare, only Banyan Vines had comparable technical strengths, but Banyan never gained a secure base. Microsoft and 3Com worked together to create a simple network operating system which formed the base of 3Com's 3+Share, Microsoft's LAN Manager and IBM's LAN Server - but none of these were particularly successful.

During the same period, Unix computer workstations from vendors such as Sun Microsystems, Hewlett-Packard, Silicon Graphics, Intergraph, NeXT and Apollo were using TCP/IP based networking. Although this market segment is now much reduced, the technologies developed in this area continue to be influential on the Internet and in both Linux and Apple Mac OS X networking—and the TCP/IP protocol has now almost completely replaced IPX, AppleTalk, NBF, and other protocols used by the early PC LANs.

## Cabling

Early LAN cabling had always been based on various grades of coaxial cable. However shielded twisted pair was used in IBM's Token Ring implementation, and in 1984 StarLAN showed the potential of simple *unshielded* twisted pair by using Cat3—the same simple cable used for telephone systems. This led to the development of 10Base-T (and its successors) and structured cabling which is still the basis of most commercial LANs today. In addition, fiber-optic cabling is increasingly used in commercial applications.

As cabling is not always possible, wireless Wi-Fi is now very common in residential premises - and elsewhere where support for mobile laptops and smartphones is important.

## Technical aspects

Network topology describes the layout pattern of interconnections between devices and network segments. Switched Ethernet has been for some time the most common Data Link Layer and Physical Layer implementation for local area networks. At the higher layers, the Internet Protocol (TCP/IP) has become the standard. Smaller LANs generally consist of one or more switches linked to each other, often at least one is connected to a router, cable modem, or ADSL modem for Internet access.

Larger LANs are characterized by their use of redundant links with switches using the spanning tree protocol to prevent loops, their ability to manage differing traffic types via quality of service (QoS), and to segregate traffic with VLANs. Larger LANs also contain a wide variety of network devices such as switches, firewalls, routers, load balancers, and sensors.<sup>[14]</sup>

LANs may have connections with other LANs via leased lines, leased services, or by tunneling across the Internet using virtual private network technologies. Depending on how the connections are established and secured in a LAN, and the distance involved, a LAN may also be classified as a metropolitan area network (MAN) or a wide area network (WAN).

## References

- [1] Gary A. Donahue (2007-06). *Network Warrior*. O'Reilly. p. 5.
- [2] Samuel F. Mendicino (1970-12-01). "Octopus: The Lawrence Radiation Laboratory Network" (<http://www.webcitation.org/5tP07Xoec>). Rogerdmoores.ca. Archived from the original (<http://www.rogerdmoores.ca/PS/OCTOA/OCTO.html>) on 2010-10-11..
- [3] "THE LAWRENCE RADIATION LABORATORY OCTOPUS". *Courant symposium series on networks* (Osti.gov). 29 Nov 1970. OSTI 4045588.
- [4] "A brief informal history of the Computer Laboratory" (<http://www.webcitation.org/5tP0nKIIL>). University of Cambridge. 20 December 2001. Archived from the original (<http://www.cl.cam.ac.uk/conference/EDSAC99/history.html>) on 2010-10-11..
- [5] "Ethernet Prototype Circuit Board" (<http://americanhistory.si.edu/collections/object.cfm?key=35&objkey=96>). Smithsonian National Museum of American History. . Retrieved 2007-09-02.
- [6] <http://www.google.com/patents?vid=4063220>
- [7] "Ethernet: Distributed Packet-Switching For Local Computer Networks" (<http://www.acm.org/classics/apr96/>). Acm.org. . Retrieved 2010-10-11.
- [8] "ARCNET Timeline" (<http://www.webcitation.org/5tP1JOSj5>). ARCNETHworks magazine. Fall 1998. Archived from the original (<http://www.arcnet.com/resources/HistoryATA.pdf>) on 2010-10-11..
- [9] Lamont Wood (2008-01-31). "The LAN turns 30, but will it reach 40?" (<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9060198>). Computerworld.com. . Retrieved 2010-10-11.
- [10] "*The Year of The LAN* is a long-standing joke, and I freely admit to being the comedian that first declared it in 1982..." ([http://books.google.co.nz/books?id=FzsEAAAAMBAJ&pg=PA45&lpg=PA45&dq=%the+year+of+the+LAN%+bogus&source=bl&ots=hGEgb2Ekvc&sig=y6XBt\\_XvpIqlq-kmVwUSRoYUCe8&hl=en&ei=6YlnTcCmNIjksQP9-tymBA&sa=X&oi=book\\_result&ct=result&resnum=1&ved=0CBgQ6AEwAA#v=onepage&q&f=false](http://books.google.co.nz/books?id=FzsEAAAAMBAJ&pg=PA45&lpg=PA45&dq=%the+year+of+the+LAN%+bogus&source=bl&ots=hGEgb2Ekvc&sig=y6XBt_XvpIqlq-kmVwUSRoYUCe8&hl=en&ei=6YlnTcCmNIjksQP9-tymBA&sa=X&oi=book_result&ct=result&resnum=1&ved=0CBgQ6AEwAA#v=onepage&q&f=false)), Robert Metcalfe, InfoWorld Dec 27, 1993
- [11] "...you will remember numerous computer magazines, over numerous years, announcing 'the year of the LAN.'" (<http://www.ibiblio.org/java/quotes1999.html>), Quotes in 1999
- [12] "...a bit like the Year of the LAN which computer industry pundits predicted for the good part of a decade..." (<http://herot.typepad.com/herot/2010/10/connected-health-symposium.html>), Christopher Herot
- [13] Wayne Spivak (2001-07-13). "Has Microsoft Ever Read the History Books?" (<http://www.webcitation.org/5tP23vwBy>). VARBusiness. Archived from the original (<http://guide.sbanetweb.com/press/varbiz07116001.html>) on 2010-10-11..
- [14] "A Review of the Basic Components of a Local Area Network (LAN)" (<http://networkbits.net/lan-components/local-area-network-lan-basic-components/>). NetworkBits.net. . Retrieved 2008-04-08.

# Campus area network

---

A **campus network**, **campus area network**, **corporate area network** or **CAN** is a computer network made up of an interconnection of local area networks (LANs) within a limited geographical area.<sup>[1][2]</sup> The networking equipments (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc.) are almost entirely owned by the campus tenant / owner: an enterprise, university, government etc.<sup>[3]</sup>

## University campuses

College or university campus area networks often interconnect a variety of buildings, including administrative buildings, academic buildings, university libraries, campus or student centers, residence halls, gymnasiums, and other outlying structures, like conference centers, technology centers, and training institutes.

Early examples include the Stanford University Network at Stanford University,<sup>[4]</sup> Project Athena at MIT,<sup>[5]</sup> and the Andrew Project at Carnegie Mellon University.<sup>[6]</sup>

## Corporate campuses

Much like a university campus network, a corporate campus network serves to connect buildings. Examples of such are the networks at Googleplex and Microsoft's campus. Campus networks are normally interconnected with high speed Ethernet links operating over optical fiber such as Gigabit Ethernet and 10 Gigabit Ethernet.

## References

- [1] Edwards, Wade. CCNP Complete Study Guide (642-801, 642-811, 642-821, 642-831). Sybex. © 2005
- [2] Long, Cormac. IP Network Design. McGraw-Hill/Osborne. © 2001.
- [3] Gary A. Donahue (2007-06). *Network Warrior*. O'Reilly. p. 5.
- [4] "Network (SUNet — The Stanford University Network)" (<http://itservices.stanford.edu/service/network>). Stanford University Information Technology Services. July 16, 2010. . Retrieved May 4, 2011.
- [5] "Athena history (1983 - present) from A to Z" (<http://web.mit.edu/acs/athena.html>). MIT. . Retrieved May 4, 2011.
- [6] N. S. Borenstein (December 1996). "CMU's Andrew project: a retrospective" (<ftp://ftp.andrew.cmu.edu/pub/AUIS/PAPERS/atk/Boren.CACM>). *Communications of the ACM* **39** (12). doi:10.1145/272682.272717. .

# Metropolitan area network

A **metropolitan area network (MAN)** is a computer network that usually spans a city or a large campus. A MAN usually interconnects a number of local area networks (LANs) using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to wide area networks (or WAN) and the Internet.

The IEEE 802-2002 standard describes a MAN as being:<sup>[1]</sup>

A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for internetworking of local networks.

Authors Kenneth C. Laudon and Jane P. Laudon (2001) of *Management Information Systems: Managing the Digital Firm 10th ed.* define a metropolitan area network as:

A Metropolitan Area Network (MAN) is a large computer network that spans a metropolitan area or campus. Its geographic scope falls between a WAN and LAN. MANs provide Internet connectivity for LANs in a metropolitan region, and connect them to wider area networks like the Internet.

It can also be used in cable television.

## Implementation

Some technologies used for this purpose are Asynchronous Transfer Mode (ATM), FDDI, and SMDS. These technologies are in the process of being displaced by Ethernet-based connections (e.g., Metro Ethernet) in most areas. MAN links between local area networks have been built without cables using either microwave, radio, or infra-red laser links. Most companies rent or lease circuits from common carriers because laying long stretches of cable can be expensive.

DQDB, Distributed-queue dual-bus, is the metropolitan area network standard for data communication. It is specified in the IEEE 802.6 standard. Using DQDB, networks can be up to 20 miles (30 km) long and operate at speeds of 34 to 155 Mbit/s.

Several notable networks started as MANs, such as the Internet peering points MAE-West, MAE-East, and the Sohonet media network.

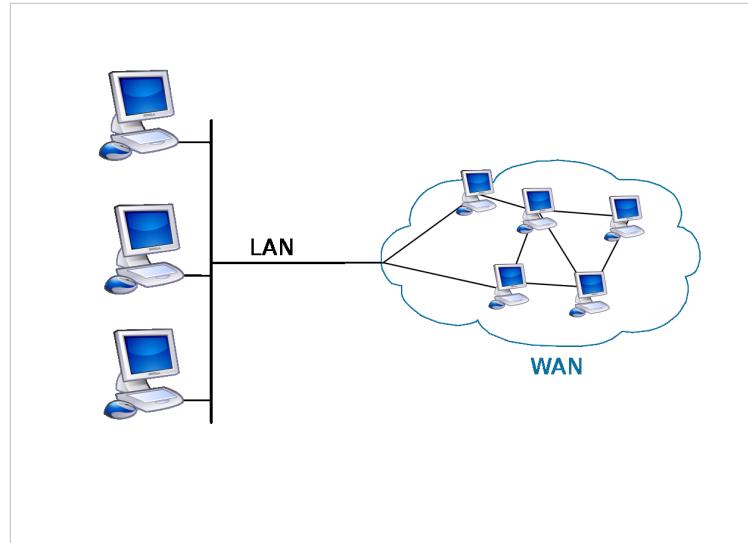
## References

[1] IEEE Std 802-2002, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture, page 1, section 1.2: "Key Concepts", "basic technologies" <http://standards.ieee.org/getieee802/download/802-2001.pdf>

# Wide area network

A **Wide Area Network** (WAN) is a telecommunication network that covers a broad area (i.e., any network that links across metropolitan, regional, or national boundaries). Business and government entities utilize WANs to relay data among employees, clients, buyers, and suppliers from various geographical locations. In essence this mode of telecommunication allows a business to effectively carry out its daily function regardless of location.<sup>[1]</sup>

This is in contrast with personal area networks (PANs), local area networks (LANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area (e.g., a city) respectively.



## Design options

The textbook definition of a WAN is a computer network spanning regions, countries, or even the world. However, in terms of the application of computer networking protocols and concepts, it may be best to view WANs as computer networking technologies used to transmit data over long distances, and between different LANs, MANs and other localised computer networking architectures. This distinction stems from the fact that common LAN technologies operating at Layer 1/2 (such as the forms of Ethernet or Wifi) are often geared towards physically localised networks, and thus cannot transmit data over tens, hundreds or even thousands of miles or kilometres.

WANs necessarily do not just connect physically disparate LANs. A CAN, for example, may have a localised backbone of a WAN technology, which connects different LANs within a campus. This could be to facilitate higher bandwidth applications, or provide better functionality for users in the CAN.

WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet. WANs are often built using leased lines. At each end of the leased line, a router connects the LAN on one side with a second router within the LAN on the other. Leased lines can be very expensive. Instead of using leased lines, WANs can also be built using less costly circuit switching or packet switching methods. Network protocols including TCP/IP deliver transport and addressing functions. Protocols including Packet over SONET/SDH, MPLS, ATM and Frame relay are often used by service providers to deliver the links that are used in WANs. X.25 was an important early WAN protocol, and is often considered to be the "grandfather" of Frame Relay as many of the underlying protocols and functions of X.25 are still in use today (with upgrades) by Frame Relay.

Academic research into wide area networks can be broken down into three areas: mathematical models, network emulation and network simulation.

Performance improvements are sometimes delivered via wide area file services or WAN optimization.

## Connection technology options

Several options are available for WAN connectivity:<sup>[2]</sup>

Option:	Description	Advantages	Disadvantages	Bandwidth range	Sample protocols used
<b>Leased line</b>	Point-to-Point connection between two computers or Local Area Networks (LANs)	Most secure	Expensive		PPP, HDLC, SDLC, HNAS
<b>Circuit switching</b>	A dedicated circuit path is created between end points. Best example is dialup connections	Less Expensive	Call Setup	28 - 144 kbit/s	PPP, ISDN
<b>Packet switching</b>	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier internetwork. Variable length packets are transmitted over Permanent Virtual Circuits (PVC) or Switched Virtual Circuits (SVC)		Shared media across link		X.25 Frame-Relay
<b>Cell relay</b>	Similar to packet switching, but uses fixed length cells instead of variable length packets. Data is divided into fixed-length cells and then transported across virtual circuits	Best for simultaneous use of voice and data	Overhead can be considerable		ATM

Transmission rates usually range from 1200 bit/s to 24 Mbit/s, although some connections such as ATM and Leased lines can reach speeds greater than 156 Mbit/s. Typical communication links used in WANs are telephone lines, microwave links & satellite channels.

Recently with the proliferation of low cost of Internet connectivity many companies and organizations have turned to VPN to interconnect their networks, creating a WAN in that way. Companies such as Cisco, New Edge Networks and Check Point offer solutions to create VPN networks.

## National area network

Some countries have nationwide computer networks, such as Kwangmyong in North Korea.

## References

- [1] Groth, David and Skandler, Toby (2009). *Network+ Study Guide, Fourth Edition*. Sybex, Inc. ISBN 0-7821-4406-3.
- [2] McQuerry, Steve (November 19, 2003). '*CCNA Self-Study: Interconnecting Cisco Network Devices (ICND), Second Edition*'. Cisco Press. ISBN 1-58705-142-7.

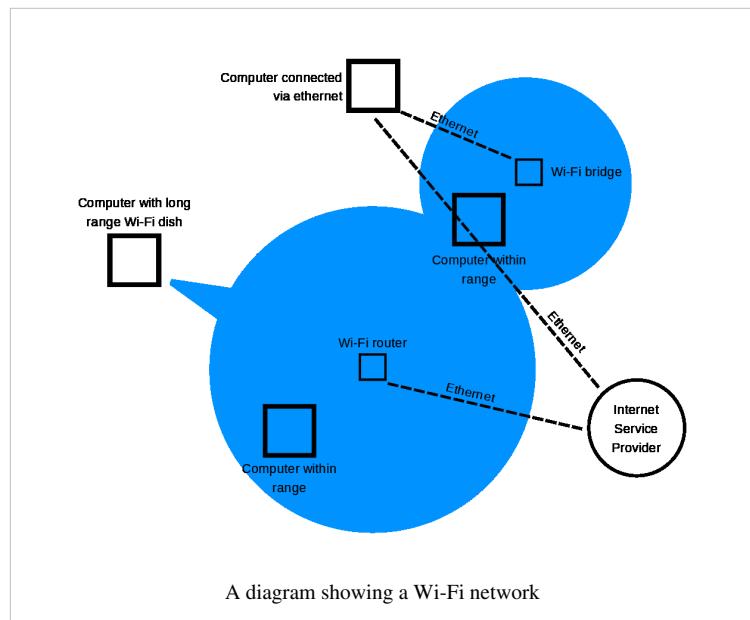
## External links

- Cisco - Introduction to WAN Technologies ([http://docwiki.cisco.com/wiki/Internetworking\\_Technology\\_Handbook#WAN\\_Technologies](http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook#WAN_Technologies))

# Wi-Fi Hotspot

A **hotspot** is a site that offers Internet access over a wireless local area network through the use of a router connected to a link to an Internet service provider. Hotspots typically use Wi-Fi technology.

Hotspots may be found in coffee shops and various other public establishments in many developed urban areas throughout the world.



## History

Public access wireless local area networks (LANs) were first proposed by Henrik Sjödin at the NetWorld+Interop conference in The Moscone Center in San Francisco in August 1993.<sup>[1]</sup> Sjödin did not use the term hotspot but referred to publicly accessible wireless LANs. Sjödin went on to found the companies PLANCOM in 1994 (for Public LAN Communications, which became MobileStar and then the HotSpot unit of T-Mobile USA) and Wayport in 1996.

The term HotSpot may have first been advanced by Nokia about five years after Sjödin first proposed the concept.

During the dot-com period in 2000, dozens of companies had the notion that Wi-Fi could become the payphone for broadband. The original notion was that users would pay for broadband access at hotspots.

Both paid and free hotspots continue to grow. Wireless networks that cover entire cities, such as municipal broadband have mushroomed.



Public park in Brooklyn, NY has free Wifi from a local corporation

## Uses

The public can use a laptop, Wi-Fi phone, or other suitable portable device to access the wireless connection (usually Wi-Fi) provided. Of the estimated 150 million laptops, 14 million PDAs, and other emerging Wi-Fi devices sold per year for the last few years, most include the Wi-Fi feature.

For venues that have broadband Internet access, offering wireless access is as simple as purchasing one access point (AP), in conjunction with a router and connecting the AP to the Internet connection. A single wireless router combining these functions may suffice.<sup>[2]</sup>

## Locations

Hotspots are often found at restaurants, train stations, airports, libraries, hotels, hospitals, coffee shops, bookstores, fuel stations, department stores, supermarkets, RV parks and campgrounds, public pay phones, and other public places. Many universities and schools have wireless networks in their campus.

## Types

### Free Wi-Fi hotspots

Free hotspots operate in two ways:

- Using an open public network is the easiest way to create a free hotSpot. All that is needed is a Wi-Fi router. Private users of wireless routers can turn off their authentication requirements, thus opening their connection, intentionally or not, for sharing by anyone in range. The disadvantage is that access to the router cannot be controlled.
- Closed public networks use a HotSpot Management System to control the HotSpot. This software runs on the router itself or an external computer. With this software, operators can authorize only specific users to access the Internet, and they often associate the free access to a menu or to a purchase limit. Operators are also now able to limit each user's available bandwidth - each user is therefore restricted to a certain speed to ensure that everyone gets a good quality service. Often this is done through Service Level Agreements.



In a public pay phone, there is also sometimes a hotspot.

### Commercial hotspots

A commercial hotspot may feature:

- A captive portal / Login Screen that users are redirected to for authentication and payment
- A payment option using credit card, PayPal, iPass, or other payment service
- A walled garden feature that allows free access to certain sites
- Service oriented provisioning to allow for improved revenue

Many services provide payment services to hotspot providers, for a monthly fee or commission from the end-user income. ZoneCD is a Linux distribution that provides payment services for hotspots who wish to deploy their own service.

Hotspots that intend to offer both fee and free internet access may want to look at Amazingports and their implementation of Service oriented provisioning

Major airports and business hotels are more likely to charge for service. Most hotels provide free service to guests; and increasingly, small airports and airline lounges offer free service.

Roaming services are expanding among major hotspot service providers. With roaming service the users of a commercial provider can have access to other provider's hotspots with extra fees, in which such a user will be usually charged on the basis of access-per-minute. Roaming agreements can be hard to negotiate with larger providers such as Boingo, so smaller hotspots usually use an aggregator such as [www.gowifi.com](http://www.gowifi.com) to access these networks.

FON is a European company that allows users to share their wireless broadband and sells excess bandwidth to outside users (Aliens). Since this may breach users terms of service, FON has agreements with many broadband providers / ISPs.

KeyWifi similarly allows users to pay the owners of connections for usage, especially during off hours. Initial service is at Queensbridge Houses in Long Island City, New York.<sup>[3]</sup>

## Billing

		Net traffic					
		low			high		
		Audio	Video	Data	Audio	Video	Data
User needs	time-critical	7	5	0	6	4	0
	not time-critical	-	-	2	-	-	2

EDCF User-Priority-List

The so called "User-Fairness-Model" <sup>[4]</sup> is a dynamic billing model, which allows a volume-based billing, with only the payload (data, video, audio) will be charged. Moreover, the tariff is classified by net traffic and user needs (Pommer, p. 116ff).

If the net traffic increases, then the user has to pay the next higher tariff class. By the way the user is asked for if he still wishes the session also by a higher traffic class. Moreover, in time-critical applications (video, audio) a higher class fare is charged, than for non time-critical applications (such as reading Web pages, e-mail).

		Net traffic	
		low	
		standard	exclusive
User needs	time-critical	standard	exclusive
	not time-critical	low priced	standard

Tariff classes of the User-Fairness-Model

The "User-fairness model" can be implemented with the help of EDCF (IEEE 802.11e). A EDCF user priority list shares the traffic in 3 access categories (data, video, audio) and user priorities (UP) (Pommer, p. 117):

- Data [UP 0|2]
- Video [UP 5|4]
- Audio [UP 7|6]

If the net traffic increases, then the frames of the particular access category (AC) are assigned a low priority value (e.g. video UP 5 to UP 4). This is also, if the data transfer is not time-critical.

## Security concerns

Some hotspots authenticate users. This does not secure the data transmission or prevent packet sniffers from allowing people to see traffic on the network.

Some vendors provide a download option that deploys WPA support. This conflicts with enterprise configurations that have solutions specific to their internal WLAN.

In order to provide robust security to hotspot users, WiFi alliance is coming up with a new hotspot program which aims to encrypt hotspot traffic with the latest WPA2 security. The program is planned to launch in the first half of 2012.

## Legal concerns

Offerers of public hotspot access may incur legal obligations, including privacy requirements and liability for use for unlawful purposes, depending on the jurisdiction. [5]

### European Union

- Data Retention Directive Hotspot owners must retain key user statistics for 12 months.
- Directive on Privacy and Electronic Communications

### United Kingdom

- Data Protection Act 1998 The hotspot owner must retain individual's information within the confines of the law.
- Digital Economy Act 2010 Deals with, amongst other things, Copyright infringement, and imposes fines of up to £250,000 for contravention.

## References

- [1] Wi-Fi Timeline [http://wifinetnews.com/archives/2002/08/wi-fi\\_timeline.html](http://wifinetnews.com/archives/2002/08/wi-fi_timeline.html)
- [2] Setting up a hotspot ([http://reviews.cnet.com/4520-6603\\_7-5023845-1.html](http://reviews.cnet.com/4520-6603_7-5023845-1.html))
- [3] <http://nyconvergence.com/2011/10/wifi-sharing-service-keywifi-to-go-live-at-queensbridge-public-housing.html> Wifi Sharing Service KeyWifi to go live at Queensbridge] NYconvergence.com
- [4] Pommer, Hermann: *Roaming zwischen Wireless Local Area Networks*. VDM Verlag, Saarbrücken 2008, ISBN 978-3-8364-8708-5.
- [5] WiFi Foundation Legal Advice <http://www.wififoundation.org/legal>

# OSI Model

## OSI model

The **Open Systems Interconnection (OSI) model** is a product of the Open Systems Interconnection effort at the International Organization for Standardization. It is a prescription of characterizing and standardizing the functions of a communications system in terms of abstraction layers. Similar communication functions are grouped into logical layers. A layer serves the layer above it and is served by the layer below it.

For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal connection on that layer.

### History

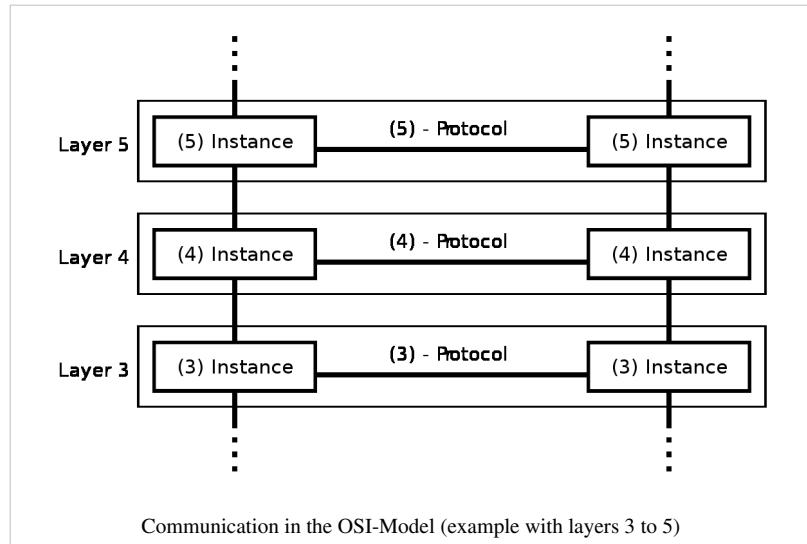
Work on a layered model of network architecture was started and the International Organization for Standardization (ISO) began to develop its OSI framework architecture. OSI had two major components: an *abstract model* of networking, called the Basic Reference Model or seven-layer model, and a set of specific protocols.

The concept of a seven-layer model was provided by the work of Charles Bachman, Honeywell Information

Services. Various aspects of OSI design evolved from experiences with the ARPANET, the fledgling Internet, NPLNET, EIN, CYCLADES network and the work in IFIP WG6.1. The new design was documented in ISO 7498 and its various addenda. In this model, a networking system was divided into layers. Within each layer, one or more entities implement its functionality. Each entity interacted directly only with the layer immediately beneath it, and provided facilities for use by the layer above it.

Protocols enabled an entity in one host to interact with a corresponding entity at the same layer in another host. Service definitions abstractly described the functionality provided to an (N)-layer by an (N-1) layer, where N was one of the seven layers of protocols operating in the local host.

The OSI standards documents are available from the ITU-T as the X.200-series of recommendations.<sup>[1]</sup> Some of the protocol specifications were also available as part of the ITU-T X series. The equivalent ISO and ISO/IEC standards for the OSI model were available from ISO, but only some of them without fees.<sup>[2]</sup>



## Description of OSI layers

According to recommendation X.200, there are seven layers, labeled 1 to 7, with layer 1 at the bottom. Each layer is generically known as an N layer. An "N+1 entity" (at layer N+1) requests services from an "N entity" (at layer N).

At each level, two entities (N-entity peers) interact by means of the N protocol by transmitting protocol data units (PDU).

A Service Data Unit (SDU) is a specific unit of data that has been passed down from an OSI layer to a lower layer, and which the lower layer has not yet encapsulated into a protocol data unit (PDU). An SDU is a set of data that is sent by a user of the services of a given layer, and is transmitted semantically unchanged to a peer service user.

The PDU at a layer N is the SDU of layer N-1. In effect the SDU is the 'payload' of a given PDU. That is, the process of changing an SDU to a PDU, consists of an encapsulation process, performed by the lower layer. All the data contained in the SDU becomes encapsulated within the PDU. The layer N-1 adds headers or footers, or both, to the SDU, transforming it into a PDU of layer N-1. The added headers or footers are part of the process used to make it possible to get data from a source to a destination.

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	End-to-end connections, reliability and flow control
Media layers	Packet/Datagram	3. Network	Path determination and logical addressing
	Frame	2. Data link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

Some orthogonal aspects, such as management and security, involve every layer.

Security services are not related to a specific layer: they can be related by a number of layers, as defined by ITU-T X.800 Recommendation.<sup>[3]</sup>

These services are aimed to improve the CIA triad (confidentiality, integrity, and availability) of transmitted data. Actually the availability of communication service is determined by network design and/or network management protocols. Appropriate choices for these are needed to protect against denial of service.

### Layer 1: physical layer

The physical layer defines electrical and physical specifications for devices. In particular, it defines the relationship between a device and a transmission medium, such as a copper or fiber optical cable. This includes the layout of pins, voltages, cable specifications, hubs, repeaters, network adapters, host bus adapters (HBA used in storage area networks) and more.

The major functions and services performed by the physical layer are:

- Establishment and termination of a connection to a communications medium.
- Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.
- Modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.

Parallel SCSI buses operate in this layer, although it must be remembered that the logical SCSI protocol is a transport layer protocol that runs over this bus. Various physical-layer Ethernet standards are also in this layer; Ethernet incorporates both this layer and the data link layer. The same applies to other local-area networks, such as token ring, FDDI, ITU-T G.hn and IEEE 802.11, as well as personal area networks such as Bluetooth and IEEE 802.15.4.

## **Layer 2: data link layer**

The data link layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer. Originally, this layer was intended for point-to-point and point-to-multipoint media, characteristic of wide area media in the telephone system. Local area network architecture, which included broadcast-capable multi-access media, was developed independently of the ISO work in IEEE Project 802. IEEE work assumed sublayer-ing and management functions not required for WAN use. In modern practice, only error detection, not flow control using sliding window, is present in data link protocols such as Point-to-Point Protocol (PPP), and, on local area networks, the IEEE 802.2 LLC layer is not used for most protocols on the Ethernet, and on other local area networks, its flow control and acknowledgment mechanisms are rarely used. Sliding window flow control and acknowledgment is used at the transport layer by protocols such as TCP, but is still used in niches where X.25 offers performance advantages.

The ITU-T G.hn standard, which provides high-speed local area networking over existing wires (power lines, phone lines and coaxial cables), includes a complete data link layer which provides both error correction and flow control by means of a selective repeat Sliding Window Protocol.

Both WAN and LAN service arrange bits, from the physical layer, into logical sequences called frames. Not all physical layer bits necessarily go into frames, as some of these bits are purely intended for physical layer functions. For example, every fifth bit of the FDDI bit stream is not used by the layer.

### **WAN protocol architecture**

Connection-oriented WAN data link protocols, in addition to framing, detect and may correct errors. They are also capable of controlling the rate of transmission. A WAN data link layer might implement a sliding window flow control and acknowledgment mechanism to provide reliable delivery of frames; that is the case for Synchronous Data Link Control (SDLC) and HDLC, and derivatives of HDLC such as LAPB and LAPD.

### **IEEE 802 LAN architecture**

Practical, connectionless LANs began with the pre-IEEE Ethernet specification, which is the ancestor of IEEE 802.3. This layer manages the interaction of devices with a shared medium, which is the function of a media access control (MAC) sublayer. Above this MAC sublayer is the media-independent IEEE 802.2 Logical Link Control (LLC) sublayer, which deals with addressing and multiplexing on multi-access media.

While IEEE 802.3 is the dominant wired LAN protocol and IEEE 802.11 the wireless LAN protocol, obsolete MAC layers include Token Ring and FDDI. The MAC sublayer detects but does not correct errors.

## **Layer 3: network layer**

The network layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network (in contrast to the data link layer which connects hosts within the same network), while maintaining the quality of service requested by the transport layer. The network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer, sending data throughout the extended network and making the Internet possible. This is a logical addressing scheme – values are chosen by the network engineer. The addressing scheme is not hierarchical.

---

The network layer may be divided into three sublayers:

1. Subnetwork access – that considers protocols that deal with the interface to networks, such as X.25;
2. Subnetwork-dependent convergence – when it is necessary to bring the level of a transit network up to the level of networks on either side
3. Subnetwork-independent convergence – handles transfer across multiple networks.

An example of this latter case is CLNP, or IPv6 ISO 8473. It manages the connectionless transfer of data one hop at a time, from end system to ingress router, router to router, and from egress router to destination end system. It is not responsible for reliable delivery to a next hop, but only for the detection of erroneous packets so they may be discarded. In this scheme, IPv4 and IPv6 would have to be classed with X.25 as subnet access protocols because they carry interface addresses rather than node addresses.

A number of layer-management protocols, a function defined in the Management Annex, ISO 7498/4, belong to the network layer. These include routing protocols, multicast group management, network-layer information and error, and network-layer address assignment. It is the function of the payload that makes these belong to the network layer, not the protocol that carries

## Layer 4: transport layer

The transport layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state- and connection-oriented. This means that the transport layer can keep track of the segments and retransmit those that fail. The transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred.

OSI defines five classes of connection-mode transport protocols ranging from class 0 (which is also known as TP0 and provides the least features) to class 4 (TP4, designed for less reliable networks, similar to the Internet). Class 0 contains no error recovery, and was designed for use on network layers that provide error-free connections. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the session layer. Also, all OSI TP connection-mode protocol classes provide expedited data and preservation of record boundaries. Detailed characteristics of TP0-4 classes are shown in the following table:<sup>[4]</sup>

Feature Name	TP0	TP1	TP2	TP3	TP4
Connection oriented network	Yes	Yes	Yes	Yes	Yes
Connectionless network	No	No	No	No	Yes
Concatenation and separation	No	Yes	Yes	Yes	Yes
Segmentation and reassembly	Yes	Yes	Yes	Yes	Yes
Error Recovery	No	Yes	Yes	Yes	Yes
Reinitiate connection (if an excessive number of PDUs are unacknowledged)	No	Yes	No	Yes	No
Multiplexing and demultiplexing over a single virtual circuit	No	No	Yes	Yes	Yes
Explicit flow control	No	No	Yes	Yes	Yes
Retransmission on timeout	No	No	No	No	Yes
Reliable Transport Service	No	Yes	No	Yes	Yes

An easy way to visualize the transport layer is to compare it with a Post Office, which deals with the dispatch and classification of mail and parcels sent. Do remember, however, that a post office manages the outer envelope of mail. Higher layers may have the equivalent of double envelopes, such as cryptographic presentation services that can be read by the addressee only. Roughly speaking, tunneling protocols operate at the transport layer, such as carrying non-IP protocols such as IBM's SNA or Novell's IPX over an IP network, or end-to-end encryption with IPsec.

While Generic Routing Encapsulation (GRE) might seem to be a network-layer protocol, if the encapsulation of the payload takes place only at endpoint, GRE becomes closer to a transport protocol that uses IP headers but contains complete frames or packets to deliver to an endpoint. L2TP carries PPP frames inside transport packet.

Although not developed under the OSI Reference Model and not strictly conforming to the OSI definition of the transport layer, the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) of the Internet Protocol Suite are commonly categorized as layer-4 protocols within OSI.

## **Layer 5: session layer**

The session layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite. The session layer is commonly implemented explicitly in application environments that use remote procedure calls. On this level, Inter-Process communication happen (SIGHUP, SIGKILL, End Process, etc.).

## **Layer 6: presentation layer**

The presentation layer establishes context between application-layer entities, in which the higher-layer entities may use different syntax and semantics if the presentation service provides a mapping between them. If a mapping is available, presentation service data units are encapsulated into session protocol data units, and passed down the stack.

This layer provides independence from data representation (e.g., encryption) by translating between application and network formats. The presentation layer transforms data into the form that the application accepts. This layer formats and encrypts data to be sent across a network. It is sometimes called the syntax layer.<sup>[5]</sup>

The original presentation structure used the basic encoding rules of Abstract Syntax Notation One (ASN.1), with capabilities such as converting an EBCDIC-coded text file to an ASCII-coded file, or serialization of objects and other data structures from and to XML.

## **Layer 7: application layer**

The application layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application-layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit. When determining resource availability, the application layer must decide whether sufficient network or the requested communication exist. In synchronizing communication, all communication between applications requires cooperation that is managed by the application layer. Some examples of application-layer implementations also include:

- On OSI stack:
  - FTAM File Transfer and Access Management Protocol
  - X.400 Mail
  - Common Management Information Protocol (CMIP)
- On TCP/IP stack:
  - Hypertext Transfer Protocol (HTTP),
  - File Transfer Protocol (FTP),

- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP).

## Cross-layer functions

There are some functions or services that are not tied to a given layer, but they can affect more than one layer. Examples include the following:

- security service (telecommunication)<sup>[3]</sup> as defined by ITU-T X.800 Recommendation.
- management functions, i.e. functions that permit to configure, instantiate, monitor, terminate the communications of two or more entities: there is a specific application layer protocol, common management information protocol (CMIP) and its corresponding service, common management information service (CMIS), they need to interact with every layer in order to deal with their instances.
- Multiprotocol Label Switching (MPLS) operates at an OSI-model layer that is generally considered to lie between traditional definitions of layer 2 (data link layer) and layer 3 (network layer), and thus is often referred to as a "layer-2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, and Ethernet frames.
- ARP is used to translate IPv4 addresses (OSI layer 3) into Ethernet MAC addresses (OSI layer 2).

## Interfaces

Neither the OSI Reference Model nor OSI protocols specify any programming interfaces, other than as deliberately abstract service specifications. Protocol specifications precisely define the interfaces between different computers, but the software interfaces inside computers, known as network sockets are implementation-specific.

For example Microsoft Windows' Winsock, and Unix's Berkeley sockets and System V Transport Layer Interface, are interfaces between applications (layer 5 and above) and the transport (layer 4). NDIS and ODI are interfaces between the media (layer 2) and the network protocol (layer 3).

Interface standards, except for the physical layer to media, are approximate implementations of OSI service specifications.

## Examples

Layer		OSI protocols	TCP/IP protocols	Signaling System 7 <sup>[6]</sup>	AppleTalk	IPX	SNA	UMTS	Misc. examples
#	Name								
7	Application	FTAM, X.400, X.500, DAP, ROSE, RTSE, ACSE <sup>[7]</sup> CMIP <sup>[8]</sup>	NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, DHCP, SMPP, SMTP, SNMP, Telnet, RIP, BGP	INAP, MAP, TCAP, ISUP, TUP	AFP, ZIP, RTMP, NBP	RIP, SAP	APPN		HL7, Modbus
6	Presentation	ISO/IEC 8823, X.226, ISO/IEC 9576-1, X.236	MIME, SSL, TLS, XDR		AFP				TDI, ASCII, EBCDIC, MIDI, MPEG

5	Session	ISO/IEC 8327, X.225, ISO/IEC 9548-1, X.235	Sockets. Session establishment in TCP, RTP		ASP, ADSP, PAP	NWLink	DLC?		Named pipes, NetBIOS, SAP, half duplex, full duplex, simplex, RPC, SOCKS
4	Transport	ISO/IEC 8073, TP0, TP1, TP2, TP3, TP4 (X.224), ISO/IEC 8602, X.234	TCP, UDP, SCTP, DCCP			DDP, SPX			NBF
3	Network	ISO/IEC 8208, X.25 (PLP), ISO/IEC 8878, X.223, ISO/IEC 8473-1, CLNP X.233.	IP, IPsec, ICMP, IGMP, OSPF	SCCP, MTP	ATP (TokenTalk or EtherTalk)	IPX		RRC (Radio Resource Control) and BMC (Broadcast/Multicast Control)	NBF, Q.931, NDP ARP (maps layer 3 to layer 2 address), IS-IS
2	Data Link	ISO/IEC 7666, X.25 (LAPB), Token Bus, X.222, ISO/IEC 8802-2 LLC Type 1 and 2 <sup>[9]</sup>	PPP, SBTM SLIP, PPTP	MTP, Q.710	LocalTalk, AppleTalk Remote Access, PPP	IEEE 802.3 framing, Ethernet II framing	SDLC	Packet Data Convergence Protocol (PDCP) <sup>[10]</sup> , LLC (Logical Link Control), MAC (Media Access Control)	802.3 (Ethernet), 802.11a/b/g/n MAC/LLC, 802.1Q (VLAN), ATM, HDP, FDDI, Fibre Channel, Frame Relay, HDLC, ISL, PPP, Q.921, Token Ring, CDP, ITU-T G.hn DLL CRC, Bit stuffing, ARQ, Data Over Cable Service Interface Specification (DOCSIS), interface bonding
1	Physical	X.25 (X.21bis, EIA/TIA-232, EIA/TIA-449, EIA-530, G.703) <sup>[9]</sup>		MTP, Q.710	RS-232, RS-422, STP, PhoneNet		Twinax	UMTS Physical layer or L1	RS-232, Full duplex, RJ45, V.35, V.34, I.430, I.431, T1, E1, 10BASE-T, 100BASE-TX, 1000BASE-T, POTS, SONET, SDH, DSL, 802.11a/b/g/n PHY, ITU-T G.hn PHY, Controller Area Network, Data Over Cable Service Interface Specification (DOCSIS)

## Comparison with TCP/IP model

In the TCP/IP model of the Internet, protocols are deliberately not as rigidly designed into strict layers as in the OSI model.<sup>[11]</sup> RFC 3439 contains a section entitled "Layering considered harmful (section link here [12])." However, TCP/IP does recognize four broad layers of functionality which are derived from the operating scope of their contained protocols, namely the scope of the software application, the end-to-end transport connection, the internetworking range, and the scope of the direct links to other nodes on the local network.

Even though the concept is different from the OSI model, these layers are nevertheless often compared with the OSI layering scheme in the following way: The Internet application layer includes the OSI application layer, presentation layer, and most of the session layer. Its end-to-end transport layer includes the graceful close function of the OSI session layer as well as the OSI transport layer. The internetworking layer (Internet layer) is a subset of the OSI network layer (see above), while the link layer includes the OSI data link and physical layers, as well as parts of OSI's network layer. These comparisons are based on the original seven-layer protocol model as defined in ISO 7498, rather than refinements in such things as the internal organization of the network layer document.

The presumably strict peer layering of the OSI model as it is usually described does not present contradictions in TCP/IP, as it is permissible that protocol usage does not follow the hierarchy implied in a layered model. Such examples exist in some routing protocols (e.g., OSPF), or in the description of tunneling protocols, which provide a link layer for an application, although the tunnel host protocol may well be a transport or even an application layer protocol in its own right.

## References

- [1] ITU-T X-Series Recommendations (<http://www.itu.int/rec/T-REC-X/en>)
- [2] "Publicly Available Standards" (<http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>). Standards.iso.org. 2010-07-30. . Retrieved 2010-09-11.
- [3] X.800 : Security architecture for Open Systems Interconnection for CCITT applications (<http://www.itu.int/rec/T-REC-X.800-199103-I-e>)
- [4] "ITU-T Recommendation X.224 (11/1995) ISO/IEC 8073" (<http://www.itu.int/rec/T-REC-X.224-199511-I/en/>). .
- [5] Grigonis, Richard (2000). *Computer telephony encyclopedia* (<http://books.google.com/books?id=cUYk0ZhOxpEC&printsec=frontcover&dq=computer+telephony+encyclopedia&ct=result#v=onepage&q&f=false>). CMP. pp. 331.. .
- [6] ITU-T Recommendation Q.1400 (03/1993) (<http://www.itu.int/rec/T-REC-Q.1400/en/>), *Architecture framework for the development of signaling and OA&M protocols using OSI concepts*, pp 4, 7.
- [7] ITU Rec. X.227 (ISO 8650), X.217 (ISO 8649)
- [8] X.700 series of recommendations from the ITU-T (in particular X.711), and ISO 9596
- [9] CISCO Cisco Systems, Inc. Internetworking Technology Handbook OSI Model Physical layer (<http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html#wp1020669>)
- [10] 3GPP TS 36.300 : E-UTRA and E-UTRAN Overall Description, Stage 2, Release 11 (<http://www.3gpp.org/ftp/Specs/html-info/36300.htm>)
- [11] RFC 3439
- [12] <http://tools.ietf.org/html/rfc3439#section-3>

## External links

- ISO/IEC standard 7498-1:1994 ([http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269\\_ISO\\_IEC\\_7498-1\\_1994\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip)) (PDF document inside ZIP archive) (requires HTTP cookies in order to accept licence agreement)
- ITU-T X.200 (the same contents as from ISO) ([http://www.itu.int/rec/dologin\\_pub.asp?lang=e&id=T-REC-X.200-199407-I!!PDF-E&type=items](http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.200-199407-I!!PDF-E&type=items))
- The ISO OSI Reference Model , Beluga graph of data units and groups of layers (<http://infchg.appspot.com/usr?at=1263939371>)
- Zimmermann, Hubert (April 1980). "OSI Reference Model — The ISO Model of Architecture for Open Systems Interconnection". *IEEE Transactions on Communications* **28** (4): 425–432. CiteSeerX: 10.1.1.136.9497 (<http://>

[citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.136.9497](http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.136.9497)).

- Cisco Systems Internetworking Technology Handbook ([http://docwiki.cisco.com/wiki/Internetworking\\_Technology\\_Handbook](http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook))
- Collection of animations and videos concerning computer networks (<http://www.khurramtanvir.com/cs460demos.php>)

## Physical Layer

---

In the seven-layer OSI model of computer networking, the **physical layer** or **layer 1** is the first (lowest) layer.<sup>[1]</sup> The implementation of this layer is often termed **PHY**.

The physical layer consists of the basic networking hardware transmission technologies of a network.<sup>[2]</sup> It is a fundamental layer underlying the logical data structures of the higher level functions in a network. Due to the plethora of available hardware technologies with widely varying characteristics, this is perhaps the most complex layer in the OSI architecture.

The physical layer defines the means of transmitting raw bits rather than logical data packets over a physical link connecting network nodes. The bit stream may be grouped into code words or symbols and converted to a physical signal that is transmitted over a hardware transmission medium. The physical layer provides an electrical, mechanical, and procedural interface to the transmission medium. The shapes and properties of the electrical connectors, the frequencies to broadcast on, the modulation scheme to use and similar low-level parameters, are specified here.

Within the semantics of the OSI network architecture, the physical layer translates logical communications requests from the data link layer into hardware-specific operations to affect transmission or reception of electronic signals.

### Physical signaling sublayer

In a local area network (LAN) or a metropolitan area network (MAN) using open systems interconnection (OSI) architecture, the *physical signaling sublayer* is the portion of the physical layer that:<sup>[3][4]</sup>

- interfaces with the data link layer's media access control (MAC) sublayer,
- performs character encoding, transmission, reception and decoding and,
- performs galvanic isolation.

### List of services

The major functions and services performed by the physical layer are:

- Bit-by-bit or symbol-by-symbol delivery
- Providing a standardized interface to physical transmission media, including
  - Mechanical specification of electrical connectors and cables, for example maximum cable length
  - Electrical specification of transmission line signal level and impedance
  - Radio interface, including electromagnetic spectrum frequency allocation and specification of signal strength, analog bandwidth, etc.
  - Specifications for IR over optical fiber or a wireless IR communication link
- Modulation
- Line coding
- Bit synchronization in synchronous serial communication
- Start-stop signalling and flow control in asynchronous serial communication
- Circuit switching

- Multiplexing
  - Establishment and termination of circuit switched connections
- Carrier sense and collision detection utilized by some level 2 multiple access protocols
- Equalization filtering, training sequences, pulse shaping and other signal processing of physical signals
- Forward error correction<sup>[5]</sup> for example bitwise convolutional coding
- Bit-interleaving and other channel coding

The physical layer is also concerned with

- Bit rate
- Point-to-point, multipoint or point-to-multipoint line configuration
- Physical network topology, for example bus, ring, mesh or star network
- Serial or parallel communication
- Simplex, half duplex or full duplex transmission mode
- Autonegotiation

## List of protocols

- Telephone network modems- V.92
- IRDA physical layer
- USB physical layer
- EIA RS-232, EIA-422, EIA-423, RS-449, RS-485
- Ethernet physical layer Including 10BASE-T, 10BASE2, 10BASE5, 100BASE-TX, 100BASE-FX, 100BASE-T, 1000BASE-T, 1000BASE-SX and other varieties
- Varieties of 802.11 Wi-Fi physical layers
- DSL
- ISDN
- T1 and other T-carrier links, and E1 and other E-carrier links
- SONET/SDH
- Optical Transport Network (OTN)
- GSM Um air interface physical layer
- Bluetooth physical layer
- ITU Recommendations: see ITU-T
- IEEE 1394 interface
- TransferJet physical layer
- Etherloop
- ARINC 818 Avionics Digital Video Bus
- G.hn/G.9960 physical layer
- CAN bus (controller area network) physical layer

## Hardware equipment (network node) examples

- Network adapter
- Repeater
- Network hub
- Modem
- Fiber Media Converter

## Relation to TCP/IP model

The TCP/IP model, defined in RFC 1122 and RFC 1123, is a high-level networking description used for the Internet and similar networks. It does not define an equivalent layer that deals exclusively with hardware-level specifications and interfaces, as this model does not concern itself directly with physical interfaces. Several RFCs mention a physical layer and data link layer, but that is in context of IEEE protocols. RFC 1122 and 1123 do not mention any physical layer functionality or physical layer standards.

## References

- [1] Banzal, Shashi (2007). *Data and Computer Network Communication* ([http://books.google.com/books?id=UD0h\\_GqgbHgC&printsec=frontcover&dq=network++guide+to+networks&src=bnr&v=onepage&q=&f=false](http://books.google.com/books?id=UD0h_GqgbHgC&printsec=frontcover&dq=network++guide+to+networks&src=bnr&v=onepage&q=&f=false)). Firewall Media. pp. 41. .
- [2] Iyengar, Shisharama (2010). *Fundamentals of Sensor Network Programming* ([http://books.google.com/books?id=UD0h\\_GqgbHgC&printsec=frontcover&dq=network++guide+to+networks&src=bnr&v=onepage&q=&f=false](http://books.google.com/books?id=UD0h_GqgbHgC&printsec=frontcover&dq=network++guide+to+networks&src=bnr&v=onepage&q=&f=false)). Wiley. pp. 136. .
- [3] This article incorporates public domain material from the General Services Administration document "Federal Standard 1037C" (<http://www.its.blrdoc.gov/fs-1037/fs-1037c.htm>).
- [4] "physical signaling sublayer (PLS)" ([http://www.tiaonline.org/market\\_intelligence/glossary/index.cfm?term=&#TC\]SR?N](http://www.tiaonline.org/market_intelligence/glossary/index.cfm?term=&#TC]SR?N) ) . Retrieved 2011-07-29.
- [5] Bertsekas, Dimitri; Gallager, Robert (1992). *Data Networks*. Prentice Hall. p. 61. ISBN 0-13-200916-1.

## External links

- Gorry Fairhurst (2001-01-01). "Physical Layer" (<http://replay.web.archive.org/20090618154921/http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/phy.html>). Archived from the original (<http://www.erg.abdn.ac.uk/users/gorry/course/phy-pages/phy.html>) on 2009-06-08.
- Physical Layer (Layer 1) ([http://www.tcpipguide.com/free/t\\_PhysicalLayerLayer1.htm](http://www.tcpipguide.com/free/t_PhysicalLayerLayer1.htm))

# Media Access Control

---

In the seven-layer OSI model of computer networking, **media access control (MAC)** data communication protocol is a sublayer of the data link layer, which itself is layer 2. The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. The hardware that implements the MAC is referred to as a *medium access controller*.

The MAC sublayer acts as an interface between the logical link control (LLC) sublayer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

## Functions performed in the MAC sublayer

According to 802.3-2002 section 4.1.4, the functions required of a MAC are:<sup>[1]</sup>

- receive/transmit normal frames
- half-duplex retransmission and backoff functions
- append/check FCS (frame check sequence)
- interframe gap enforcement
- discard malformed frames
- append(tx)/remove(rx) preamble, SFD, and padding
- half-duplex compatibility: append(tx)/remove(rx) MAC address

In 100Mbps and faster MACs, the MAC address is not actually handled in the MAC layer. Doing so would make it impossible to implement IP because the ARP(Address Resolution Protocol) layer of IP-Ethernet needs access to the MAC address.

## Addressing mechanism

In 100Mbit/s and faster Ethernet MACs, there is no required addressing mechanism. However, the MAC address inherited from the original MAC layer specification is used in many higher level protocols such as Internet Protocol (IP) over Ethernet.

The local network address used in IP-Ethernet is called MAC address because it historically was part of the MAC layer in early Ethernet implementations. The MAC layer's addressing mechanism is called physical address or MAC address. A MAC address is a unique serial number. Once a MAC address has been assigned to a particular network interface (typically at time of manufacture), that device should be uniquely identifiable amongst all other network devices in the world. This guarantees that each device in a network will have a different MAC address (analogous to a street address). This makes it possible for data packets to be delivered to a destination within a subnetwork, i.e. hosts interconnected by some combination of repeaters, hubs, bridges and switches, but not by IP routers. Thus, when an IP packet reaches its destination (sub)network, the destination IP address (a layer 3 or network layer concept) is resolved with the Address Resolution Protocol for IPv4, or by Neighbor Discovery Protocol (IPv6) into the MAC address (a layer 2 concept) of the destination host.

An example of a physical network is an Ethernet network, perhaps extended by wireless local area network (WLAN) access points and WLAN network adapters, since these share the same 48-bit MAC address hierarchy as Ethernet.

A MAC layer is not required in full-duplex point-to-point communication, but address fields are included in some point-to-point protocols for compatibility reasons.

## Channel access control mechanism

The channel access control mechanisms provided by the MAC layer are also known as a multiple access protocol. This makes it possible for several stations connected to the same physical medium to share it. Examples of shared physical media are bus networks, ring networks, hub networks, wireless networks and half-duplex point-to-point links. The multiple access protocol may detect or avoid data packet collisions if a packet mode contention based channel access method is used, or reserve resources to establish a logical channel if a circuit switched or channelization based channel access method is used. The channel access control mechanism relies on a physical layer multiplex scheme.

The most widespread multiple access protocol is the contention based CSMA/CD protocol used in Ethernet networks. This mechanism is only utilized within a network collision domain, for example an Ethernet bus network or a hub-based star topology network. An Ethernet network may be divided into several collision domains, interconnected by bridges and switches.

A multiple access protocol is not required in a switched full-duplex network, such as today's switched Ethernet networks, but is often available in the equipment for compatibility reasons.

## Common multiple access protocols

Examples of common packet mode multiple access protocols for wired multi-drop networks are:

- CSMA/CD (used in Ethernet and IEEE 802.3)
- Token bus (IEEE 802.4)
- Token ring (IEEE 802.5)
- Token passing (used in FDDI)

Examples of common multiple access protocols that may be used in packet radio wireless networks are:

- CSMA/CA (used in IEEE 802.11/WiFi WLANs)
- Slotted ALOHA
- Dynamic TDMA

and main]] (MS-ALOHA)

- CDMA
- OFDMA

## References

[1] IEEE 802.3

This article is based on material taken from the Free On-line Dictionary of Computing prior to 1 November 2008 and incorporated under the "relicensing" terms of the GFDL, version 1.3 or later.

# Logical Link Control

---

In the seven-layer OSI model of computer networking, the **logical link control (LLC)** data communication protocol layer is the upper sublayer of the data link layer, which is itself layer 2. The LLC sublayer provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX, Decnet and Appletalk) to coexist within a multipoint network and to be transported over the same network media. It can also provide flow control and automatic repeat request (ARQ) error management mechanisms.

The LLC sublayer acts as an interface between the media access control (MAC) sublayer and the network layer.

## Operation

The LLC sublayer is primarily concerned with:

- Multiplexing protocols transmitted over the MAC layer (when transmitting) and decoding them (when receiving).
- Providing node-to-node flow and error control

In today's networks, flow control and error management is typically taken care of by a transport layer protocol such as the TCP protocol, or by some application layer protocol, in an end-to-end fashion, i.e. retransmission is done from source to end destination. This implies that the need for LLC sublayer flow control and error management has reduced. LLC is consequently only a multiplexing feature in today's link layer protocols. An LLC header tells the data link layer what to do with a packet once a frame is received. It works like this: A host will receive a frame and look in the LLC header to find out to what protocol stack the packet is destined - for example, the IP protocol at the network layer or IPX. However, today most non-IP network protocols are abandoned.

## Application examples

### X.25 and LAPB

An LLC sublayer was a key component in early packet switching networks such as X.25 networks with the LAPB data link layer protocol, where flow control and error management were carried out in a node-to-node fashion, meaning that if an error was detected in a frame, the frame was retransmitted from one switch to next instead. This extensive handshaking between the nodes made the networks slow.

### Local area network (LAN) and metropolitan area network (MAN) protocols

The IEEE 802.2 standard specifies LLC sublayer for all IEEE 802 local area networks, such as IEEE 802.3/Ethernet (if the EtherType field is used), IEEE 802.5, and IEEE 802.11, and in some non-IEEE 802 networks such as FDDI.

### Ethernet

Since bit errors are very rare in wired networks, Ethernet does not provide flow control or automatic repeat request (ARQ), meaning that incorrect packets are detected but only cancelled, not retransmitted (except in case of collisions detected by the CSMA/CD MAC layer protocol). Instead, retransmissions rely on higher layer protocols.

As the EtherType in an Ethernet II framing formatted frame is used to multiplex different protocols on top of the Ethernet MAC header it can be seen as LLC identifier. However, If Ethernet is used without EtherType field, Ethernet is considered as lacking LLC sublayer.

## Wireless LAN

In wireless communications, bit errors are very common. In wireless networks such as IEEE 802.11, flow control and error management is part of the CSMA/CA MAC protocol, and not part of the LLC layer. The LLC sublayer follows the IEEE 802.2 standard.

## HDLC

Some non-IEEE 802 protocols can be thought of as being split into MAC and LLC layers. For example, while HDLC specifies both MAC functions (framing of packets) and LLC functions (protocol multiplexing, flow control, detection, and error control through a retransmission of dropped packets when indicated), some protocols such as Cisco HDLC can use HDLC-like packet framing and their own LLC protocol.

## PPP and modems

Over telephone network modems, PPP link layer protocols can be considered as a LLC protocol, providing multiplexing, but it does not provide flow control and error management. In a telephone network, bit errors might be common, meaning that error management is crucial, but that is today provided by modern protocols. Today's modem protocols have inherited LLC features from the older LAPM link layer protocol, made for modem communication in old X.25 networks.

## Cellular systems

The GPRS LLC layer also does ciphering and deciphering of SN-PDU (SNDCP) packets.

## Power lines

Another example of a data link layer which is split between LLC (for flow and error control) and MAC (for multiple access) is the ITU-T G.hn standard, which provides high-speed local area networking over existing home wiring (power lines, phone lines and coaxial cables).

# Data Link Layer

---

In the seven-layer OSI model of computer networking, the **data link layer** is **layer 2**. In TCP/IP reference model, it corresponds to, or is part of the link layer.

The data link layer is the protocol layer that transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment.<sup>[1]</sup> The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC and ADCCP for point-to-point (dual-node) connections.

The data link layer is concerned with local delivery of frames between devices on the same LAN. Data-link frames, as these protocol data units are called, do not cross the boundaries of a local network. Inter-network routing and global addressing are higher layer functions, allowing data-link protocols to focus on local delivery, addressing, and media arbitration. In this way, the data link layer is analogous to a neighborhood traffic cop; it endeavors to arbitrate between parties contending for access to a medium.

When devices attempt to use a medium simultaneously, frame collisions occur. Data-link protocols specify how devices detect and recover from such collisions, and may provide mechanisms to reduce or prevent them.

Delivery of frames by layer-2 devices is effected through the use of unambiguous hardware addresses. A frame's header contains source and destination addresses that indicate which device originated the frame and which device is expected to receive and process it. In contrast to the hierarchical and routable addresses of the network layer, layer-2 addresses are flat, meaning that no part of the address can be used to identify the logical or physical group to which the address belongs.

The data link thus provides data transfer across the physical link. That transfer can be reliable or unreliable; many data-link protocols do not have acknowledgments of successful frame reception and acceptance, and some data-link protocols might not even have any form of checksum to check for transmission errors. In those cases, higher-level protocols must provide flow control, error checking, and acknowledgments and retransmission.

In some networks, such as IEEE 802 local area networks, the data link layer is described in more detail with media access control (MAC) and logical link control (LLC) sublayers; this means that the IEEE 802.2 LLC protocol can be used with all of the IEEE 802 MAC layers, such as Ethernet, token ring, IEEE 802.11, etc., as well as with some non-802 MAC layers such as FDDI. Other data-link-layer protocols, such as HDLC, are specified to include both sublayers, although some other protocols, such as Cisco HDLC, use HDLC's low-level framing as a MAC layer in combination with a different LLC layer. In the ITU-T G.hn standard, which provides a way to create a high-speed (up to 1 Gigabit/s) Local area network using existing home wiring (power lines, phone lines and coaxial cables), the data link layer is divided into three sub-layers (application protocol convergence, logical link control and medium access control).

Within the semantics of the OSI network architecture, the data-link-layer protocols respond to service requests from the network layer and they perform their function by issuing service requests to the physical layer.

## Models of communication

### Sublayers of the data link layer

The data link layer has two sublayers: *logical link control* (LLC) and *media access control* (MAC).<sup>[2]</sup>

#### Logical link control sublayer

The uppermost sublayer, LLC, multiplexes protocols running atop the data link layer, and optionally provides flow control, acknowledgment, and error notification. The LLC provides addressing and control of the data link. It specifies which mechanisms are to be used for addressing stations over the transmission medium and for controlling the data exchanged between the originator and recipient machines.

#### Media access control sublayer

MAC may refer to the sublayer that determines who is allowed to access the media at any one time (usually CSMA/CD). Other times it refers to a frame structure with MAC addresses inside.

There are generally two forms of media access control: distributed and centralized. Both of these may be compared to communication between people. In a network made up of people speaking, i.e. a conversation, we look for clues from our fellow talkers to see if any of them appear to be about to speak. If two people speak at the same time, they will back off and begin a long and elaborate game of saying "no, you first".

The Media Access Control sublayer also determines where one frame of data ends and the next one starts – frame synchronization. There are four means of frame synchronization: time based, character counting, byte stuffing and bit stuffing.

- The *time based* approach simply puts a specified amount of time between frames. The major drawback of this is that new gaps can be introduced or old gaps can be lost due to external influences.
- *Character counting* simply notes the count of remaining characters in the frame's header. This method, however, is easily disturbed if this field gets faulty in some way, thus making it hard to keep up synchronization.
- *Byte stuffing* precedes the frame with a special byte sequence such as DLE STX and succeeds it with DLE ETX. Appearances of DLE (byte value 0x10) have to be escaped with another DLE. The start and stop marks are detected at the receiver and removed as well as the inserted DLE characters.
- Similarly, *bit stuffing* replaces these start and end marks with flag consisting of a special bit pattern (e.g. a 0, six 1 bits and a 0). Occurrences of this bit pattern in the data to be transmitted is avoided by inserting a bit. To use the example where the flag is 01111110, a 0 is inserted after 5 consecutive 1's in the data stream. The flags and the inserted 0's are removed at the receiving end. This makes for arbitrary long frames and easy synchronization for the recipient. Note that this stuffed bit is added even if the following data bit is 0, which could not be mistaken for a sync sequence, so that the receiver can unambiguously distinguish stuffed bits from normal bits.

### List of data-link-layer services

- Encapsulation of network layer data packets into frames
- Frame synchronization
- Logical link control (LLC) sublayer:
  - Error control (automatic repeat request, ARQ), in addition to ARQ provided by some transport-layer protocols, to forward error correction (FEC) techniques provided on the physical layer, and to error-detection and packet canceling provided at all layers, including the network layer. Data-link-layer error control (i.e. retransmission of erroneous packets) is provided in wireless networks and V.42 telephone network modems, but not in LAN protocols such as Ethernet, since bit errors are so uncommon in short wires. In that case, only error detection and canceling of erroneous packets are provided.

- Flow control, in addition to the one provided on the transport layer. Data-link-layer error control is not used in LAN protocols such as Ethernet, but in modems and wireless networks.
- Media access control (MAC) sublayer:
  - Multiple access protocols for channel-access control, for example CSMA/CD protocols for collision detection and retransmission in Ethernet bus networks and hub networks, or the CSMA/CA protocol for collision avoidance in wireless networks.
  - Physical addressing (MAC addressing)
  - LAN switching (packet switching) including MAC filtering and spanning tree protocol
  - Data packet queueing or scheduling
  - Store-and-forward switching or cut-through switching
  - Quality of Service (QoS) control
  - Virtual LANs (VLAN)

## Protocol examples

- Address Resolution Protocol (ARP)
- ARCnet
- ATM
- Cisco Discovery Protocol (CDP)
- Controller Area Network (CAN)
- Econet
- Ethernet
- Ethernet Automatic Protection Switching (EAPS)
- Fiber Distributed Data Interface (FDDI)
- Frame Relay
- High-Level Data Link Control (HDLC)
- IEEE 802.2 (provides LLC functions to IEEE 802 MAC layers)
- IEEE 802.11 wireless LAN
- LattisNet
- Link Access Procedures, D channel (LAPD)
- LocalTalk
- Multiprotocol Label Switching (MPLS)
- Nortel Discovery Protocol (NDP)
- Split multi-link trunking (SMLT)
- Point-to-Point Protocol (PPP)
- Serial Line Internet Protocol (SLIP) (obsolete)
- Spanning Tree Protocol
- StarLan
- Token ring
- Unidirectional Link Detection (UDLD)
- and most forms of serial communication.

## Interfaces

The data link layer is often implemented in software as a "network card driver". The operating system will have a defined software interface between the data link and the network transport stack above. This interface is not a layer itself, but rather a definition for interfacing between layers.

## Relation to TCP/IP model

In the frame work of the TCP/IP (Internet Protocol Suite) model, OSI's data link layer, in addition to other components, is contained in TCP/IP's lowest layer, the link layer. The Internet Protocol's link layer only concerns itself with hardware issues to the point of obtaining hardware addresses for locating hosts on a physical network link and transmitting data frames onto the link. Thus, the link layer is broader in scope and encompasses all methods that affect the local link, which is the group of connections that are limited in scope to other nodes on the local access network.

The TCP/IP model is not a top/down comprehensive design reference for networks. It was formulated for the purpose of illustrating the logical groups and scopes of functions needed in the design of the suite of internetworking protocols of TCP/IP, as needed for the operation of the Internet. In general, direct or strict comparisons of the OSI and TCP/IP models should be avoided, because the layering in TCP/IP is not a principal design criterion and in general considered to be "harmful" (RFC 3439). In particular, TCP/IP does not dictate a strict hierarchical sequence of encapsulation requirements, as is attributed to OSI protocols.

## References

- [1] "What is layer 2, and Why Should You Care?" (<http://www.accel-networks.com/blog/2009/09/what-is-layer-2-and-why-should-you-care.html>). accel-networks.com. . Retrieved 2009-09-29.
- [2] Regis J. Bates and Donald W. Gregory (2007). *Voice & data communications handbook* (<http://books.google.com/books?id=eq1kRHdyXSUC&pg=PA45>) (5th ed.). McGraw-Hill Professional. p. 45. ISBN 978-0-07-226335-0. .

## External links

- "DataLink layer simulation in C#." ([http://www.codeproject.com/KB/IP/DataLink\\_Simulator.aspx](http://www.codeproject.com/KB/IP/DataLink_Simulator.aspx))

# Network Layer

---

In the seven-layer OSI model of computer networking, the **network layer** is **layer 3**. The network layer is responsible for packet forwarding including routing through intermediate routers, whereas the data link layer is responsible for media access control, flow control and error checking.

The network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination host via one or more networks while maintaining the quality of service functions.

Functions of the network layer include:

- Connection model: connectionless communication

For example, IP is connectionless, in that a datagram can travel from a sender to a recipient without the recipient having to send an acknowledgement. Connection-oriented protocols exist at other, higher layers of that model.

- Host addressing

Every host in the network must have a unique address that determines where it is. This address is normally assigned from a hierarchical system, so you can be "Fred Murphy" to people in your house, "Fred Murphy, 1 Main Street" to Dubliners, or "Fred Murphy, 1 Main Street, Dublin" to people in Ireland, or "Fred Murphy, 1 Main Street, Dublin, Ireland" to people anywhere in the world. On the Internet, addresses are known as Internet Protocol (IP) addresses.

- Message forwarding

Since many networks are partitioned into subnetworks and connect to other networks for wide-area communications, networks use specialized hosts, called gateways or routers to forward packets between networks. This is also of interest to mobile applications, where a user may move from one location to another, and it must be arranged that his messages follow him. Version 4 of the Internet Protocol (IPv4) was not designed with this feature in mind, although mobility extensions exist. IPv6 has a better designed solution.

Within the service layering semantics of the OSI network architecture the network layer responds to service requests from the transport layer and issues service requests to the data link layer.

## Protocols

- IPv4/IPv6, Internet Protocol
- DVMRP, Distance Vector Multicast Routing Protocol
- ICMP, Internet Control Message Protocol
- IGMP, Internet Group Multicast Protocol
- PIM-SM, Protocol Independent Multicast Sparse Mode
- PIM-DM, Protocol Independent Multicast Dense Mode
- IPsec, Internet Protocol Security
- IPX, Internetwork Packet Exchange
- RIP, Routing Information Protocol
- DDP, Datagram Delivery Protocol
- RSMLT Routed-SMLT
- Shortest Path Bridging

## Relation to TCP/IP model

The TCP/IP model describes the protocols used by the Internet.<sup>[1]</sup> This model has a layer called the Internet layer, located above the link layer. In many textbooks and other secondary references the Internet layer is equated with OSI's network layer. However, this comparison is misleading as the allowed characteristics of protocols (e.g., whether they are connection-oriented or connection-less) placed into these layers are different in the two models. The Internet layer of TCP/IP is in fact only a subset of functionality of the network layer. It only describes one type of network architecture, the Internet.

In general, direct or strict comparisons between these models should be avoided, since the layering in TCP/IP is not a principal design criterion and the Internet Engineering Task Force (IETF) considers it "harmful".<sup>[2]</sup>

## References

[1] RFC 1122

[2] RFC 3439

- Tanenbaum, Andrew S. (2003). *Computer networks*. Upper Saddle River, New Jersey: Prentice Hall. ISBN 0-13-066102-3.

## External links

- OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection (<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.136.9497&rep=rep1&type=pdf>), Hubert Zimmermann, IEEE Transactions on Communications, vol. 28, no. 4, April 1980, pp. 425 – 432. (PDF-Datei; 776 kB)

# Transport Layer

---

In computer networking, the **transport layer** or **layer 4** provides end-to-end communication services for applications<sup>[1]</sup> within a layered architecture of network components and protocols. The transport layer provides convenient services such as connection-oriented data stream support, reliability, flow control, and multiplexing.

Transport layers are contained in both the TCP/IP model (RFC 1122),<sup>[2]</sup> which is the foundation of the Internet, and the Open Systems Interconnection (OSI) model of general networking. The definitions of the transport layer are slightly different in these two models. This article primarily refers to the TCP/IP model, in which TCP is largely for a convenient application programming interface to internet hosts, as opposed to the OSI-model definition of the transport layer.

The most well-known transport protocol is the Transmission Control Protocol (TCP). It lent its name to the title of the entire Internet Protocol Suite, *TCP/IP*. It is used for connection-oriented transmissions, whereas the connectionless User Datagram Protocol (UDP) is used for simpler messaging transmissions. TCP is the more complex protocol, due to its stateful design incorporating reliable transmission and data stream services. Other prominent protocols in this group are the Datagram Congestion Control Protocol (DCCP) and the Stream Control Transmission Protocol (SCTP).

## Services

There are many services that can be optionally provided by a transport-layer protocol, and different protocols may or may not implement them.

- Connection-oriented communication: Interpreting the connection as a data stream can provide many benefits to applications. It is normally easier to deal with than the underlying connection-less models, such as the Transmission Control Protocol's underlying Internet Protocol model of datagrams.
- Byte orientation: Rather than processing the messages in the underlying communication system format, it is often easier for an application to process the data stream as a sequence of bytes. This simplification helps applications work with various underlying message formats.
- Same order delivery: The network layer doesn't generally guarantee that packets of data will arrive in the same order that they were sent, but often this is a desirable feature. This is usually done through the use of segment numbering, with the receiver passing them to the application in order. This can cause head-of-line blocking.
- Reliability: Packets may be lost during transport due to network congestion and errors. By means of an error detection code, such as a checksum, the transport protocol may check that the data is not corrupted, and verify correct receipt by sending an ACK or NACK message to the sender. Automatic repeat request schemes may be used to retransmit lost or corrupted data.
- flow control: The rate of data transmission between two nodes must sometimes be managed to prevent a fast sender from transmitting more data than can be supported by the receiving data buffer, causing a buffer overrun. This can also be used to improve efficiency by reducing buffer underrun.
- Congestion avoidance: Congestion control can control traffic entry into a telecommunications network, so as to avoid congestive collapse by attempting to avoid oversubscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. For example, automatic repeat requests may keep the network in a congested state; this situation can be avoided by adding congestion avoidance to the flow control, including slow-start. This keeps the bandwidth consumption at a low level in the beginning of the transmission, or after packet retransmission.
- Multiplexing: Ports can provide multiple endpoints on a single node. For example, the name on a postal address is a kind of multiplexing, and distinguishes between different recipients of the same location. Computer applications will each listen for information on their own ports, which enables the use of more than one network service at the same time. It is part of the transport layer in the TCP/IP model, but of the session layer in the OSI model.

## Analysis

The transport layer is responsible for delivering data to the appropriate application process on the host computers. This involves statistical multiplexing of data from different application processes, i.e. forming data packets, and adding source and destination port numbers in the header of each transport-layer data packet. Together with the source and destination IP address, the port numbers constitutes a network socket, i.e. an identification address of the process-to-process communication. In the OSI model, this function is supported by the session layer.

Some transport-layer protocols, for example TCP, but not UDP, support virtual circuits, i.e. provide connection oriented communication over an underlying packet oriented datagram network. A byte-stream is delivered while hiding the packet mode communication for the application processes. This involves connection establishment, dividing of the data stream into packets called segments, segment numbering and reordering of out-of order data.

Finally, some transport-layer protocols, for example TCP, but not UDP, provide end-to-end reliable communication, i.e. error recovery by means of error detecting code and automatic repeat request (ARQ) protocol. The ARQ protocol also provides flow control, which may be combined with congestion avoidance.

UDP is a very simple protocol, and does not provide virtual circuits, nor reliable communication, delegating these functions to the application program. UDP packets are called datagrams, rather than segments.

---

TCP is used for many protocols, including HTTP web browsing and email transfer. UDP may be used for multicasting and broadcasting, since retransmissions are not possible to a large amount of hosts. UDP typically gives higher throughput and shorter latency, and is therefore often used for real-time multimedia communication where packet loss occasionally can be accepted, for example IP-TV and IP-telephony, and for online computer games.

In many non-IP-based networks, for example X.25, Frame Relay and ATM, the connection oriented communication is implemented at network layer or data link layer rather than the transport layer. In X.25, in telephone network modems and in wireless communication systems, reliable node-to-node communication is implemented at lower protocol layers.

The OSI model defines five classes of transport protocols: *TP0*, providing the least error recovery, to *TP4*, which is designed for less reliable networks.

## Protocols

The exact definition of what qualifies as a transport-layer protocol is not firm. The following is a short list:

- ATP, AppleTalk Transaction Protocol
- CUDP, Cyclic UDP
- DCCP, Datagram Congestion Control Protocol
- FCP, Fiber Channel Protocol
- IL, IL Protocol
- NBF, NetBIOS Frames protocol
- RDP, Reliable Datagram Protocol
- SCTP, Stream Control Transmission Protocol
- SPX, Sequenced Packet Exchange
- SST, Structured Stream Transport
- TCP, Transmission Control Protocol
- UDP, User Datagram Protocol
- UDP Lite
- μTP, Micro Transport Protocol

## Comparison of transport-layer protocols

Feature Name	UDP	UDP Lite	TCP	SCTP	DCCP	RUDP
Packet header size	8 bytes	8 bytes	20–60 bytes	12 bytes	12 or 16 bytes	
Transport-layer packet entity	Datagram	Datagram	Segment	Datagram	Datagram	Datagram
Connection oriented	No	No	Yes	Yes	Yes	Yes
Reliable transport	No	No	Yes	Yes	No	Yes
Unreliable transport	Yes	Yes	No	Yes	Yes	Yes
Preserve message boundary	Yes	Yes	No	Yes	Yes	Yes
Ordered delivery	No	No	Yes	Yes	No	Yes
Unordered delivery	Yes	Yes	No	Yes	Yes	Yes
Data checksum	Optional	Yes	Yes	Yes	Yes	Unsure
Checksum size (bits)	16	16	16	32	16	Unsure
Partial checksum	No	Yes	No	No	Yes	No
Path MTU	No	No	Yes	Yes	Yes	Unsure

Flow control	No	No	Yes	Yes	No	Yes
Congestion control	No	No	Yes	Yes	Yes	Unsure
ECN support	No	No	Yes	Yes	Yes	
Multiple streams	No	No	No	Yes	No	No
Multi-homing support	No	No	No	Yes	No	No
Bundling / Nagle	No	No	Yes	Yes	No	Unsure
NAT friendly <sup>[3]</sup>	Yes	Yes	Yes	Yes <sup>[4]</sup>	Yes	Yes

## Comparison of OSI transport protocols

The OSI model defines five classes of connection-mode transport protocols designated class 0 (TP0) to class 4 (TP4). Class 0 contains no error recovery, and was designed for use on network layers that provide error-free connections. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the session layer. All OSI connection-mode protocol classes provide expedited data and preservation of record boundaries. Detailed characteristics of the classes are shown in the following table:<sup>[5]</sup>

Service	TP0	TP1	TP2	TP3	TP4
Connection oriented network	Yes	Yes	Yes	Yes	Yes
Connectionless network	No	No	No	No	Yes
Concatenation and separation	No	Yes	Yes	Yes	Yes
Segmentation and reassembly	Yes	Yes	Yes	Yes	Yes
Error Recovery	No	Yes	No	Yes	Yes
Reinitiate connection (if an excessive number of PDUs are unacknowledged)	No	Yes	No	Yes	No
multiplexing and demultiplexing over a single virtual circuit	No	No	Yes	Yes	Yes
Explicit flow control	No	No	Yes	Yes	Yes
Retransmission on timeout	No	No	No	No	Yes
Reliable Transport Service	No	Yes	No	Yes	Yes

## References

- [1] RFC 1122, §1.1.3. "The transport layer provides end-to-end communication services for applications."
- [2] RFC 1122, Requirements for Internet Hosts – Communication Layers, IETF, R. Braden (Editor), October 1989
- [3] RFC 3235, Network Address Translator (NAT)-Friendly Application Design Guidelines. D. Senie. January 2002.
- [4] Hayes, D.; But, J., *Alias\_sctp Version 0.2: SCTP NAT implementation in IPFW* (<http://caia.swin.edu.au/reports/081128A/CAIA-TR-081128A.pdf>),
- [5] "ITU-T Recommendation X.224 (11/1995) ISO/IEC 8073" (<http://www.itu.int/rec/T-REC-X.224-199511-I/en/>). .

# Session Layer

---

In the seven-layer OSI model of computer networking, the **session layer is layer 5**.

The session layer provides the mechanism for opening, closing and managing a session between end-user application processes, i.e., a semi-permanent dialogue. Communication sessions consist of requests and responses that occur between applications. Session-layer services are commonly used in application environments that make use of remote procedure calls (RPCs).

An example of a session-layer protocol is the OSI protocol suite session-layer protocol, also known as X.235 or ISO 8327. In case of a connection loss this protocol may try to recover the connection. If a connection is not used for a long period, the session-layer protocol may close it and re-open it. It provides for either full duplex or half-duplex operation and provides synchronization points in the stream of exchanged messages.<sup>[1]</sup>

Other examples of session layer implementations include Zone Information Protocol (ZIP) – the AppleTalk protocol that coordinates the name binding process, and Session Control Protocol (SCP) – the DECnet Phase IV session-layer protocol.

Within the service layering semantics of the OSI network architecture, the session layer responds to service requests from the presentation layer and issues service requests to the transport layer.

## Services

- Authentication
- Permissions
- Session restoration (checkpointing and recovery)

The session layer of the OSI model is responsible for session checkpointing and recovery. It allows information of different streams, perhaps originating from different sources, to be properly combined or synchronized.

An example application is web conferencing, in which the streams of audio and video must be synchronous to avoid so-called lip synch problems. Floor control ensures that the person displayed on screen is the current speaker.

Another application is in live TV programs, where streams of audio and video need to be seamlessly merged and transitioned from one to the other to avoid silent airtime or excessive overlap.

## Protocols

- ADSP, AppleTalk Data Stream Protocol
- ASP, AppleTalk Session Protocol
- H.245, Call Control Protocol for Multimedia Communication
- ISO-SP, OSI session-layer protocol (X.225, ISO 8327)
- iSNS, Internet Storage Name Service
- L2F, Layer 2 Forwarding Protocol
- L2TP, Layer 2 Tunneling Protocol
- NetBIOS, Network Basic Input Output System
- PAP, Password Authentication Protocol
- PPTP, Point-to-Point Tunneling Protocol
- RPC, Remote Procedure Call Protocol
- RTCP, Real-time Transport Control Protocol
- SMPP, Short Message Peer-to-Peer
- SCP, Session Control Protocol
- SOCKS, the SOCKS internet protocol, see Internet socket

- ZIP, Zone Information Protocol
- SDP, Sockets Direct Protocol

## Comparison with TCP/IP model

The TCP/IP reference model does not concern itself with the OSI model's details of application or transport protocol semantics and therefore does not consider a session layer. OSI's session management in connection with the typical transport protocols (TCP, SCTP), is contained in the transport-layer protocols, or otherwise considered the realm of the application layer protocols. TCP/IP's layers are *descriptions* of operating scopes (application, host-to-host, network, link) and not detailed *prescriptions* of operating procedures or data semantics.

## References

[1] ITU-T Recommendation X.225 (<http://www.itu.int/rec/T-REC-X.225/en/>)

# Presentation Layer

---

In the seven-layer OSI model of computer networking, the **presentation layer** is **layer 6** and serves as the data translator for the network.<sup>[1][2]</sup> It is sometimes called the syntax layer.<sup>[3]</sup>

## Description

The presentation layer is responsible for the delivery and formatting of information to the application layer for further processing or display.<sup>[4]</sup> It relieves the application layer of concern regarding syntactical differences in data representation within the end-user systems. An example of a presentation service would be the conversion of an EBCDIC-coded text computer file to an ASCII-coded file.

The presentation layer is the lowest layer at which application programmers consider data structure and presentation, instead of simply sending data in form of datagrams or packets between hosts. This layer deals with issues of string representation - whether they use the Pascal method (an integer length field followed by the specified amount of bytes) or the C/C++ method (null-terminated strings, e.g. "thisisastring\0"). The idea is that the application layer should be able to point at the data to be moved, and the presentation layer will deal with the rest.

Serialization of complex data structures into flat byte-strings (using mechanisms such as TLV or XML) can be thought of as the key functionality of the presentation layer.

Encryption is typically done at this level too, although it can be done on the application, session, transport, or network layers, each having its own advantages and disadvantages.<sup>[1]</sup> Decryption is also handled at the presentation layer. For example, when logging off bank account sites the presentation layer will decrypt the data as it is received.<sup>[1]</sup> Another example is representing structure, which is normally standardized at this level, often by using XML. As well as simple pieces of data, like strings, more complicated things are standardized in this layer. Two common examples are 'objects' in object-oriented programming, and the exact way that streaming video is transmitted.

In many widely used applications and protocols, no distinction is made between the presentation and application layers. For example, HyperText Transfer Protocol (HTTP), generally regarded as an application-layer protocol, has presentation-layer aspects such as the ability to identify character encoding for proper conversion, which is then done in the application layer.

Within the service layering semantics of the OSI network architecture, the presentation layer responds to service requests from the application layer and issues service requests to the session layer.

## Services

- Data conversion<sup>[2]</sup>
- Character code translation<sup>[2]</sup>
- Compression<sup>[2]</sup>
- Encryption and Decryption<sup>[2]</sup>

## Sublayers

The presentation layer can be composed of two sublayers: common application service element (CASE) and specific application service element (SASE).<sup>[5]</sup>

### CASE

The common application service element sublayer provides services for the application layer and request services from the session layer. It provides support for common application services, such as:

- ACSE (Association Control Service Element)<sup>[5]</sup>
- ROSE (Remote Operation Service Element)
- CCR (Commitment Concurrency and Recovery)
- RTSE (Reliable Transfer Service Element)

### SASE

The specific application service element sublayer provides application specific services (protocols), such as

- FTAM (File Transfer, Access and Manager)
- VT (Virtual Terminal)
- MOTIS (Message Oriented Text Interchange Standard)
- CMIP (Common Management Information Protocol)
- JTM (Job Transfer and Manipulation) a former OSI standard<sup>[6]</sup>
- MMS (Manufacturing Messaging Service)
- RDA (Remote Database Access)
- DTP (Distributed Transaction Processing)

## Protocols

Other protocols sometimes considered at this level (though perhaps not strictly adhering to the OSI model) include:

- Apple Filing Protocol (AFP)
- Independent Computing Architecture (ICA), the Citrix system core protocol
- Lightweight Presentation Protocol (LPP)
- NetWare Core Protocol (NCP)
- Network Data Representation (NDR)
- Telnet (a remote terminal access protocol)
- eXternal Data Representation (XDR)
- X.25 Packet Assembler/Disassembler Protocol (PAD)

## References

- [1] Dean, Tamara (2010). *Network+ Guide to Networks* ([http://books.google.com/books?id=UD0h\\_GqgbHgC&printsec=frontcover&dq=network++guide+to+networks&src=bmrr#v=onepage&q&f=false](http://books.google.com/books?id=UD0h_GqgbHgC&printsec=frontcover&dq=network++guide+to+networks&src=bmrr#v=onepage&q&f=false)). Delmar. pp. 44–47..
- [2] Microsoft TechNet (<http://technet.microsoft.com/en-us/library/cc959885.aspx>)
- [3] Grigoris, Richard (2000). *Computer telephony encyclopedia* (<http://books.google.com/books?id=cUYk0ZhOxpEC&printsec=frontcover&dq=computer+telephony+encyclopedia#v=onepage&q&f=false>). CMP. pp. 331..
- [4] [http://www.linfo.org/presentation\\_layer.html](http://www.linfo.org/presentation_layer.html) Linux Information Project
- [5] Hura, Gurdeep (2001). "Application Layer" ([http://books.google.com/books?id=BViV0PoH\\_voC&lpg=PA711](http://books.google.com/books?id=BViV0PoH_voC&lpg=PA711)). *Data and Computer Communications: Networking and Internetworking*. CRC Press LLC. pp. 710–712. .
- [6] <http://www.furniss.co.uk/jtm/index.html>

# Application Layer

---

In TCP/IP, the application layer contains all protocols and methods that fall into the realm of process-to-process communications across an Internet Protocol (IP) network. Application layer methods use the underlying transport layer protocols to establish host-to-host connections.

The Internet protocol suite (TCP/IP) and the Open Systems Interconnection model (OSI model) of computer networking each specify a group of protocols and methods identified by the name **application layer**.

In the OSI model, the definition of its application layer is narrower in scope, explicitly distinguishing additional functionality above the transport layer at two additional levels, the session layer and the presentation layer. OSI specifies strict modular separation of functionality at these layers and provides protocol implementations for each layer.

## TCP/IP protocols

The following protocols are explicitly mentioned in RFC 1123 (1989), describing the application layer of the Internet protocol suite.<sup>[1]</sup>

- Remote login category
  - Telnet
- File transfer category
  - FTP
  - TFTP
- Electronic mail category
  - SMTP
  - IMAP
  - POP
- Support services category
  - DNS
  - RARP
  - BOOTP
  - SNMP
  - CMOT

## Other protocol examples

- 9P, Plan 9 from Bell Labs distributed file system protocol
- AFP,
- APPC, Advanced Program-to-Program Communication
- AMQP, Advanced Message Queuing Protocol
- BitTorrent
- Atom Publishing Protocol
- CFDP, Coherent File Distribution Protocol
- CoAP, Constrained Application Protocol
- DDS, Data Distribution Service
- DeviceNet
- eDonkey
- ENRP, Endpoint Handlespace Redundancy Protocol
- FastTrack (KaZaa, Grokster, iMesh)
- Finger, User Information Protocol
- Freenet
- FTAM, File Transfer Access and Management
- Gopher, Gopher protocol
- HL7, Health Level Seven
- HTTP, HyperText Transfer Protocol
- H.323, Packet-Based Multimedia Communications System
- IRCP, Internet Relay Chat Protocol
- Kademlia
- KAP, Anonymous File Transfer over UDP/IP (KickAss Protocol)
- LDAP, Lightweight Directory Access Protocol
- LPD, Line Printer Daemon Protocol
- MIME (S-MIME), Multipurpose Internet Mail Extensions and Secure MIME
- Modbus
- Netconf
- NFS, Network File System
- NIS, Network Information Service
- NNTP, Network News Transfer Protocol
- NTCIP, National Transportation Communications for Intelligent Transportation System Protocol
- NTP, Network Time Protocol
- OSCAR, AOL Instant Messenger Protocol
- PNRP, Peer Name Resolution Protocol
- RDP, Remote Desktop Protocol
- RELP, Reliable Event Logging Protocol
- Rlogin, Remote Login in UNIX Systems
- RPC, Remote Procedure Call
- RTMP, Real Time Messaging Protocol
- RTP, Real-time Transport Protocol
- RTPS, Real Time Publish Subscribe
- RTSP, Real Time Streaming Protocol
- SAP, Session Announcement Protocol
- SDP, Session Description Protocol
- SIP, Session Initiation Protocol

- SLP, Service Location Protocol
- SMB, Server Message Block
- SNTP, Simple Network Time Protocol
- SOCKS, the SOCKS internet protocol
- SSH, Secure Shell
- SSMS, Secure SMS Messaging Protocol
- TCAP, Transaction Capabilities Application Part
- TDS, Tabular Data Stream
- TSP, Time Stamp Protocol
- VTP, Virtual Terminal Protocol
- Whois (and RWhois), Remote Directory Access Protocol
- WebDAV
- X.400, Message Handling Service Protocol
- X.500, Directory Access Protocol (DAP)
- XMPP, Extensible Messaging and Presence Protocol

## References

[1] Robert Braden, ed. (October 1989). "RFC 1123: Requirements for Internet Hosts – Application and Support" (<http://tools.ietf.org/html/rfc1123>). Network Working Group of the IETF..

## External links

- How The Application Layer Works (<http://learn-networking.com/tcp-ip/how-the-application-layer-works>)  
(refers to the Internet Protocol Suite)

---

# IEEE 802.1

---

## IEEE 802.1D

---

**802.1D** is the IEEE MAC Bridges standard which includes Bridging, Spanning Tree and others. It is standardized by the IEEE 802.1 working group. It includes details specific to linking many of the other 802 projects including the widely deployed 802.3 (ethernet), 802.11 (Wi-Fi) and 802.16 (WiMax) standards.

VLANs (virtual LANs) are not part of 802.1D, but specified in 802.1Q.

Publishing history:

- 1990 — Original publication (802.1D-1990), based on the ISO/IEC 10038 standard
- 1998 — Revised version (802.1D-1998), incorporating the extensions 802.1p, P802.12e, 802.1j and 802.6k.
- 2004 — Revised version (802.1D-2004), incorporating the extensions 802.11c, 802.1t and 802.1w, which were separately published in 2001, and removing the original Spanning tree protocol, instead incorporating the Rapid Spanning Tree Protocol (RSTP) from 802.1w.
- 2012 — Shortest Path Bridging, IEEE 802.1aq
  - 2004 — Small amendment to add in 802.17 bridging support<sup>[1]</sup>
  - 2007 — Small amendment to add in 802.16 bridging support<sup>[2]</sup>

## References

- 802.1D MAC Bridges Standard<sup>[3]</sup>
- 802.1D Status<sup>[4]</sup>

[1] GetIEEE802 Download (<http://standards.ieee.org/getieee802/download/802.17a-2004.pdf>)

[2] GetIEEE802 Download (<http://standards.ieee.org/getieee802/download/802.16k-2007.pdf>)

[3] <http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>

[4] <http://standards.ieee.org/cgi-bin/status?Designation:%20802.1D>

# Link Layer Discovery Protocol

The **Link Layer Discovery Protocol (LLDP)** is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet.<sup>[1]</sup> The protocol is formally referred to by the IEEE as *Station and Media Access Control Connectivity Discovery* specified in standards document **IEEE 802.1AB**.<sup>[2]</sup>

LLDP performs functions similar to several proprietary protocols, such as the Cisco Discovery Protocol, Extreme Discovery Protocol, Nortel Discovery Protocol (also known as SONMP), and Microsoft's Link Layer Topology Discovery (LLTD).

## Frame structure

LLDP information is sent by devices from each of their interfaces at a fixed interval, in the form of an Ethernet frame. Each frame contains one LLDP Data Unit (LLDPDU). Each LLDPDU is a sequence of type-length-value (TLV) structures.

The Ethernet frame used in LLDP has its destination MAC address typically set to a special multicast address that 802.1D-compliant bridges do not forward<sup>[3]</sup> Other multicast and unicast destination addresses are permitted. The EtherType field is set to 0x88cc.

Each LLDP frame starts with the following mandatory TLVs: *Chassis ID*, *Port ID*, and *Time-to-Live*. The mandatory TLVs are followed by any number of optional TLVs. The frame ends with a special TLV, named *end of LLDPDU* in which both the *type* and *length* fields are 0.

Accordingly, an Ethernet frame containing an LLDPDU has the following structure:

### LLDP Ethernet frame structure

Preamble	Destination MAC	Source MAC	Ethertype	Chassis ID TLV	Port ID TLV	Time to live TLV	Optional TLVs	End of LLDPDU TLV	Frame check sequence
	01:80:c2:00:00:0e, or 01:80:c2:00:00:03, or 01:80:c2:00:00:00	Station's address	0x88CC	Type=1	Type=2	Type=3	Zero or more complete TLVs	Type=0, Length=0	

Each of the TLV components has the following basic structure:

### TLV structure

Type	Length	Value
7 bits	9 bits	0-510 octets

Custom TLVs,<sup>[4]</sup> are supported via a TLV type 127. The value of a custom TLV starts with a 24-bit organizationally unique identifier and a 1 byte organizationally specific subtype followed by data. The basic format for an organizationally specific TLV is show below:

### Organizationally specific TLV

Type	Length	Organizationally unique identifier (OUI)	Organizationally defined subtype	Organizationally defined information string
7 bits—127	9 bits	24 bits	8 bits	0-507 octets

According to IEEE Std 802.1AB, §9.6.1.3, "The Organizationally Unique Identifier shall contain the organization's OUI as defined in IEEE Std 802-2001." Each organization is responsible for managing their subtypes.

## Information gathered

Information gathered with LLDP is stored in the device as a management information database (MIB) and can be queried with the Simple Network Management Protocol (SNMP) as specified in RFC 2922. The topology of an LLDP-enabled network can be discovered by *crawling* the hosts and querying this database. Information that may be retrieved include:

- System name and description
- Port name and description
- VLAN name
- IP management address
- System capabilities (switching, routing, etc.)
- MAC/PHY information
- MDI power
- Link aggregation

## Media endpoint discovery extension

*Media Endpoint Discovery* is an enhancement of LLDP, known as **LLDP-MED**, that provides the following facilities:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Differentiated services (Diffserv) settings) enabling plug and play networking.
- Device location discovery to allow creation of location databases and, in the case of Voice over Internet Protocol (VoIP), Enhanced 911 services.
- Extended and automated power management of Power over Ethernet (PoE) end points.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

The LLDP-MED protocol extension was formally approved and published as the standard ANSI/TIA-1057 by the Telecommunications Industry Association (TIA) in April 2006.<sup>[5]</sup>

## Applications

The Link Layer Discovery Protocol may be used as a component in network management and monitoring applications. One such example is its use in data center bridging requirements.<sup>[6]</sup>

The Data Center Bridging Capabilities Exchange Protocol (DCBX) is a discovery and capability exchange protocol that is used for conveying capabilities and configuration of the above features between neighbors to ensure consistent configuration across the network.<sup>[7]</sup>

## Notes

- [1] "802.1AB-REV - Station and Media Access Control Connectivity Discovery" (<http://www.ieee802.org/1/pages/802.1AB-rev.html>). IEEE. . Retrieved 2009-10-17.
- [2] "IEEE standard 802.1AB-2009" (<http://standards.ieee.org/getieee802/download/802.1AB-2009.pdf>). .
- [3] IEEE 802.1AB-2009 suggests three such addresses, 01:80:c2:00:00:0e, 01:80:c2:00:00:03 and 01:80:c2:00:00:00.
- [4] Termed *Organizationally Specific TLVs* by IEEE 802.1AB
- [5] "ANSI/TIA-1057 standard" ([http://www.tiaonline.org/standards/technology/voip/documents/ANSI-TIA-1057\\_final\\_for\\_publication.pdf](http://www.tiaonline.org/standards/technology/voip/documents/ANSI-TIA-1057_final_for_publication.pdf)). (PDF). .
- [6] "Data Center Bridging Task Group" (<http://www.ieee802.org/1/pages/dcbridges.html>). . Retrieved 2012-03-10.
- [7] Intel, Cisco, Nuova Systems. "DCB Capabilities Exchange Protocol Specification, Rev 1.0" ([http://download.intel.com/technology/eedc/dcb\\_cep\\_spec.pdf](http://download.intel.com/technology/eedc/dcb_cep_spec.pdf)). Intel Corporation. .

## References

### External links

- IEEE 802.1AB (LLDP) Specification (<http://standards.ieee.org/getieee802/download/802.1AB-2005.pdf>)
- Tutorial on LLDP (<http://www.eetimes.com/design/communications-design/4009357/>  
Tutorial-on-the-Link-Layer-Discovery-Protocol)
- IEEE standard 802.1AB document history (<http://www.ieee802.org/1/pages/802.1ab.html>)
- The Wireshark Wiki LLDP Page (<http://wiki.wireshark.org/LinkLayerDiscoveryProtocol>)
- OpenLLDP, Open Source LLDP Project (<http://openlldp.sourceforge.net>)
- LLDPD, Open Source LLDP Project (<https://trac.luffy.cx/lldpd/>)
- ladvd, Open Source LLDP Project (<http://blinkenlights.nl/software/ladvd/>)
- Comparison of LLDP daemons (<http://www.kempgen.net/voip/lldp-agents.html>)

# Spanning tree protocol

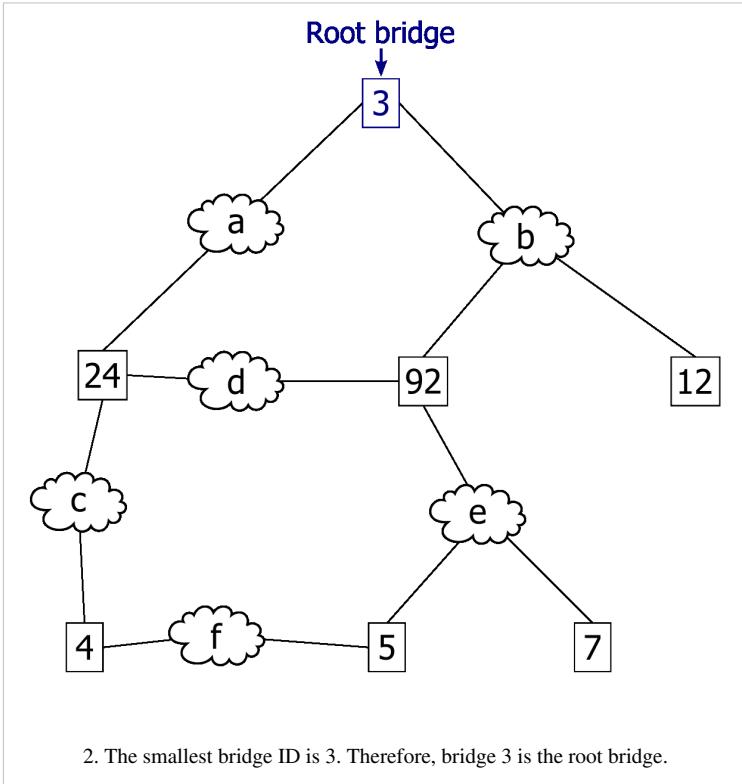
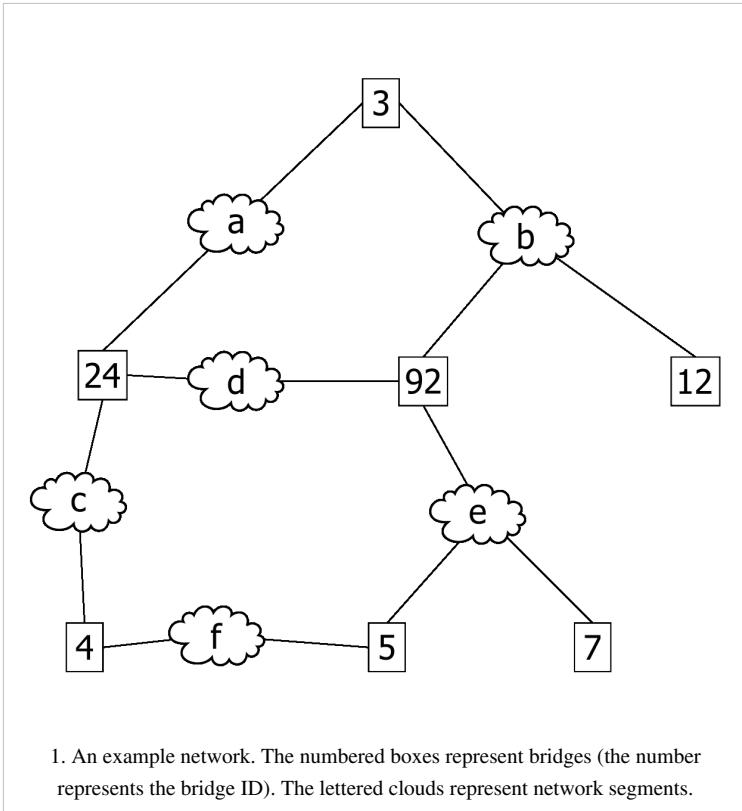
The **Spanning Tree Protocol (STP)** is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

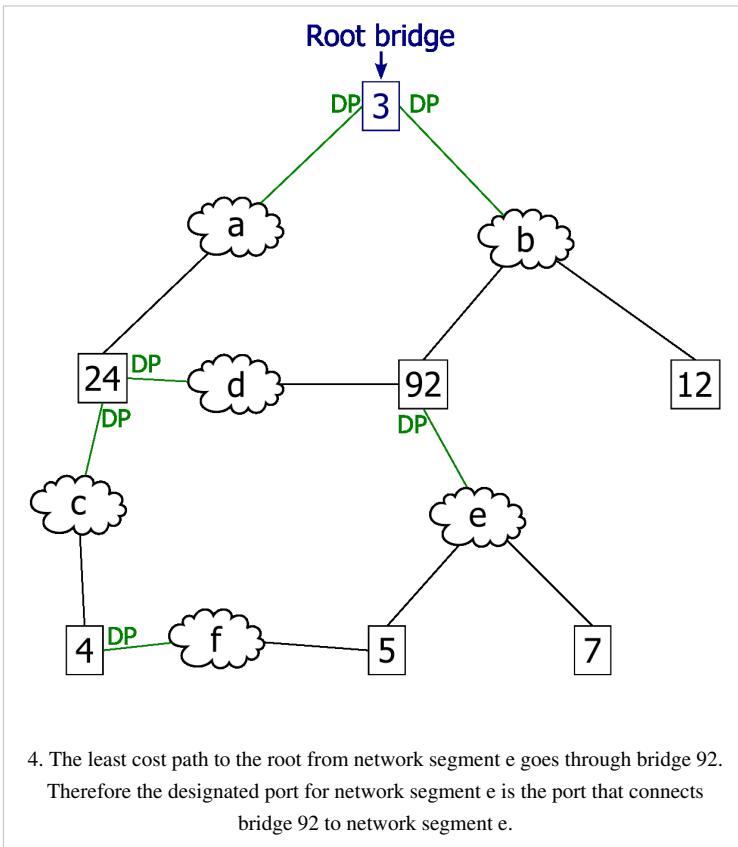
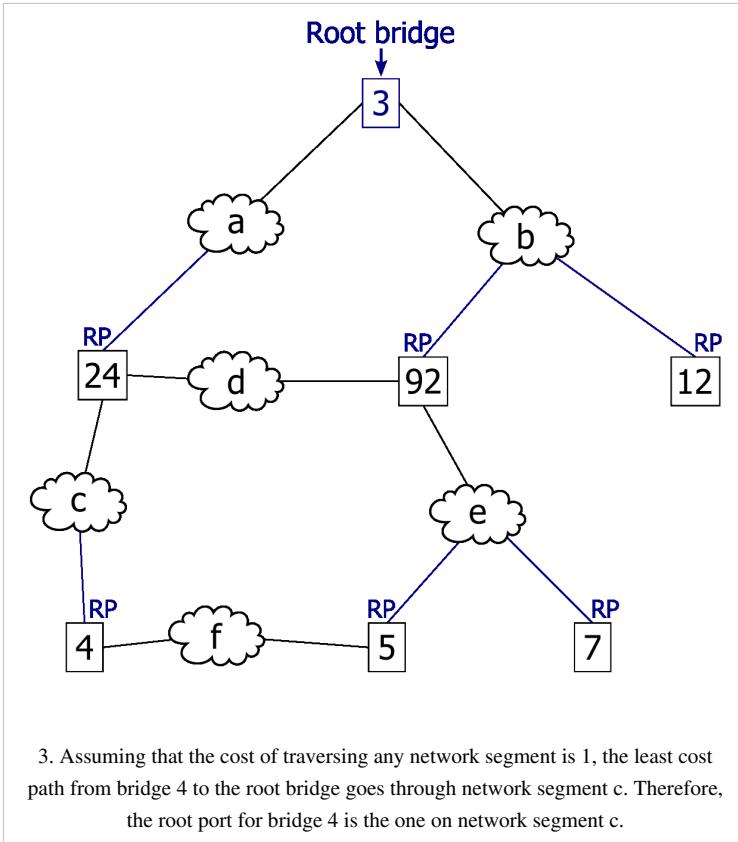
Spanning Tree Protocol (STP) is standardized as IEEE 802.1D. As the name suggests, it creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

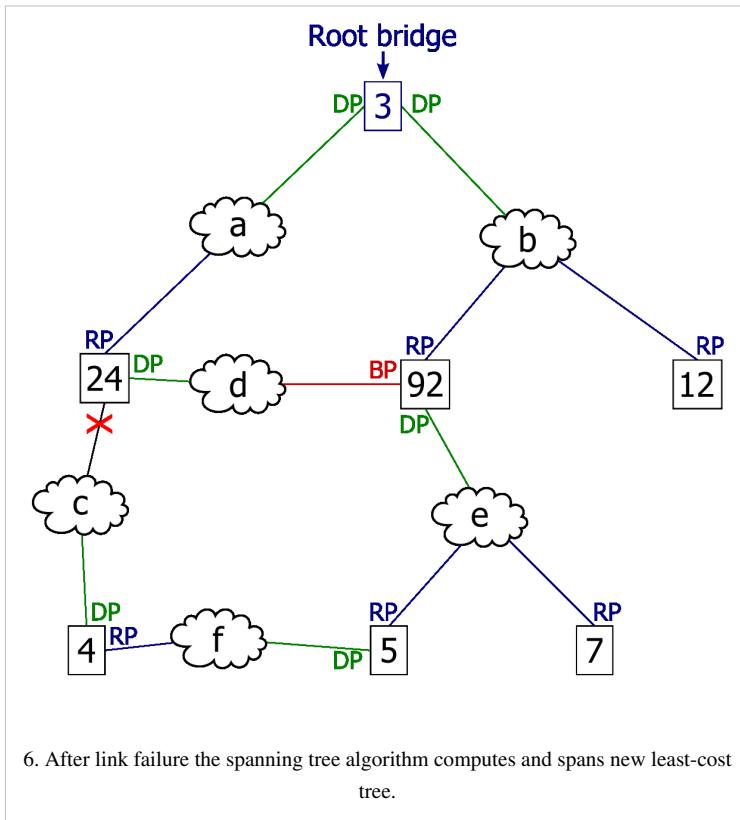
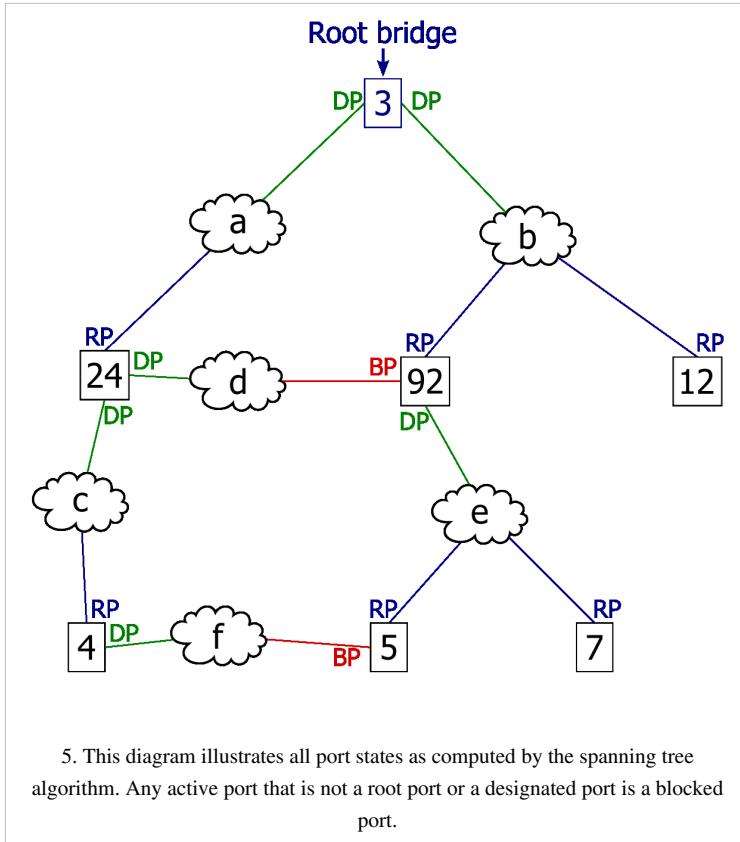
STP is based on an algorithm invented by Radia Perlman while working for Digital Equipment Corporation.<sup>[1][2]</sup>

### Protocol operation

The collection of bridges in a local area network (LAN) can be depicted as a graph whose nodes are bridges and LAN segments (or cables), and whose edges are the interfaces connecting the bridges to the segments. To break loops in the LAN while maintaining access to all LAN segments, the bridges collectively compute a spanning tree. The spanning tree is not necessarily a minimum cost spanning tree. A network administrator can reduce the cost of a spanning tree, if necessary, by altering some of the configuration parameters in such a way as to affect the choice of the root of the spanning tree. The spanning tree that the bridges compute using the Spanning Tree Protocol can be determined using the following rules. The example network at the right, below, will be used to illustrate the rules.







**Select a root bridge.** The *root bridge* of the spanning tree is the bridge with the smallest (lowest) bridge ID. Each bridge has a configurable priority number and a MAC Address; the bridge ID contains both numbers combined together - BID + MAC (32768.0200.0000.1111). The Bridge priority default is 32768 and can only be configured in

multiples of 4096. To compare two bridge IDs, the priority is compared first, as if looking at a real number anything less than 32768...will become the target of being the root. If two bridges have equal priority then the MAC addresses are compared; for example, if switches A (MAC=0200.0000.1111) and B (MAC=0200.0000.2222) both have a priority of 32768 then switch A will be selected as the root bridge. If the network administrators would like switch B to become the root bridge, they must set its priority to be less than 32768 or configure the spanning tree a root primary/secondary. When configuring the root primary and root secondary the switch will automatically change the priority accordingly, 24577 and 28673 respectively with the default configuration.

**Determine the least cost paths to the root bridge.** The computed spanning tree has the property that messages from any connected device to the root bridge traverse a least cost path, i.e., a path from the device to the root that has minimum cost among all paths from the device to the root. The cost of traversing a path is the sum of the costs of the segments on the path. Different technologies have different default costs for network segments. An administrator can configure the cost of traversing a particular network segment. The property that messages always traverse least-cost paths to the root is guaranteed by the following two rules.

*Least cost path from each bridge.* After the root bridge has been chosen, each bridge determines the cost of each possible path from itself to the root. From these, it picks one with the smallest cost (a least-cost path). The port connecting to that path becomes the *root port* (RP) of the bridge.

*Least cost path from each network segment.* The bridges on a network segment collectively determine which bridge has the least-cost path from the network segment to the root. The port connecting this bridge to the network segment is then the *designated port* (DP) for the segment.

**Disable all other root paths.** Any active port that is not a root port or a designated port is a *blocked port* (BP).

**Modifications in case of ties.** The above rules over-simplify the situation slightly, because it is possible that there are ties, for example, two or more ports on a single bridge are attached to least-cost paths to the root or two or more bridges on the same network segment have equal least-cost paths to the root. To break such ties:

*Breaking ties for root ports.* When multiple paths from a bridge are least-cost paths, the chosen path uses the neighbor bridge with the lower bridge ID. The root port is thus the one connecting to the bridge with the lowest bridge ID. For example, in figure 3, if switch 4 was connected to network segment d instead of segment c, there would be two paths of length 2 to the root, one path going through bridge 24 and the other through bridge 92. Because there are two least cost paths, the lower bridge ID (24) would be used as the tie-breaker in choosing which path to use.

*Breaking ties for designated ports.* When more than one bridge on a segment leads to a least-cost path to the root, the bridge with the lower bridge ID is used to forward messages to the root. The port attaching that bridge to the network segment is the *designated port* for the segment. In figure 4, there are two least cost paths from network segment d to the root, one going through bridge 24 and the other through bridge 92. The lower bridge ID is 24, so the tie breaker dictates that the designated port is the port through which network segment d is connected to bridge 24. If bridge IDs were equal, then the bridge with the lowest MAC address would have the designated port. In either case, the loser sets the port as being blocked.

*The final tie-breaker.* In some cases, there may still be a tie, as when two bridges are connected by multiple cables. In this case, multiple ports on a single bridge are candidates for root port. In this case, the path which passes through the port on the neighbor bridge that has the lowest port identifier [Port priority(default=128) + Port number] is used.

In summary, the sequence of events to determine the best received BPDU (which is your best path to the root) is

1. lowest root bridge id
2. lowest root path cost
3. lowest sender bridge id
4. lowest sender port id

## Data rate and STP path cost

Data rate	STP Cost (802.1D-1998)	RSTP Cost (802.1D-2004 / 802.1w) <sup>[3]</sup>
4 Mbit/s	250	5,000,000
10 Mbit/s	100	2,000,000
16 Mbit/s	62	1,250,000
100 Mbit/s	19	200,000
1 Gbit/s	4	20,000
2 Gbit/s	3	10,000
10 Gbit/s	2	2,000

## Bridge Protocol Data Units

The above rules describe one way of determining what spanning tree will be computed by the algorithm, but the rules as written require knowledge of the entire network. The bridges have to determine the root bridge and compute the port roles (root, designated, or blocked) with only the information that they have. To ensure that each bridge has enough information, the bridges use special data frames called **Bridge Protocol Data Units** (BPDUs) to exchange information about bridge IDs and root path costs.

A bridge sends a BPDU frame using the unique MAC address of the port itself as a source address, and a destination address of the STP multicast address 01:80:C2:00:00:00.

There are three types of BPDUs:

- Configuration BPDU (CBPDU), used for Spanning Tree computation
- Topology Change Notification (TCN) BPDU, used to announce changes in the network topology
- Topology Change Notification Acknowledgment (TCA)

BPDUs are exchanged regularly (every 2 seconds by default) and enable switches to keep track of network changes and to start and stop forwarding at ports as required.

When a device is first attached to a switch port, it will not immediately start to forward data. It will instead go through a number of states while it processes BPDUs and determines the topology of the network. When a host is attached such as a computer, printer or server the port will always go into the forwarding state, albeit after a delay of about 30 seconds while it goes through the listening and learning states (see below). The time spent in the listening and learning states is determined by a value known as the forward delay (default 15 seconds and set by the root bridge). However, if instead another *switch* is connected, the port may remain in blocking mode if it is determined that it would cause a loop in the network. Topology Change Notification (TCN) BPDUs are used to inform other switches of port changes. TCNs are injected into the network by a non-root switch and propagated to the root. Upon receipt of the TCN, the root switch will set a Topology Change flag in its normal BPDUs. This flag is propagated to all other switches to instruct them to rapidly age out their forwarding table entries.

### STP switch port states:

- **Blocking** - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state. Prevents the use of looped paths.
- **Listening** - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state. It does not populate the MAC address table and it does not forward frames.
- **Learning** - While the port does not yet forward frames it does learn source addresses from frames received and adds them to the filtering database (switching database). It populates the MAC Address table, but does not

forward frames.

- **Forwarding** - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.
- **Disabled** - Not strictly part of STP, a network administrator can manually disable a port

To prevent the delay when connecting hosts to a switch and during some topology changes, Rapid STP was developed and standardized by IEEE 802.1w, which allows a switch port to rapidly transition into the forwarding state during these situations.

## Bridge Protocol Data Unit fields

The bridge ID, or BID, is a field inside a BPDU packet. It is eight bytes in length. The first two bytes are the Bridge Priority, an unsigned integer of 0-65,535. The last six bytes are a MAC address supplied by the switch. In the event that MAC Address Reduction is used, the first two bytes are used differently. The first four bits are a configurable priority, and the last twelve bits carry either the VLAN ID or MSTP instance number.

## Evolutions and extensions

The first spanning tree protocol was invented in 1985 at the Digital Equipment Corporation by Radia Perlman.<sup>[1]</sup> In 1990, the IEEE published the first standard for the protocol as 802.1D,<sup>[4]</sup> based on the algorithm designed by Perlman. Subsequent versions were published in 1998<sup>[5]</sup> and 2004,<sup>[6]</sup> incorporating various extensions.

Although the purpose of a standard is to promote interworking of equipment from different vendors, different implementations of a standard are not guaranteed to work, due for example to differences in default timer settings. The IEEE encourages vendors to provide a "Protocol Implementation Conformance Statement", declaring which capabilities and options have been implemented,<sup>[6]</sup> to help users determine whether different implementations will interwork correctly.

Also, the original Perlman-inspired Spanning Tree Protocol, called DEC STP, is not a standard and differs from the IEEE version in message format as well as timer settings. Some bridges implement both the IEEE and the DEC versions of the Spanning Tree Protocol, but their interworking can create issues for the network administrator, as illustrated by the problem discussed in an on-line Cisco document.<sup>[7]</sup>

## Rapid Spanning Tree Protocol

In 2001, the IEEE introduced Rapid Spanning Tree Protocol (RSTP) as 802.1w. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP.

While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within  $3 \times \text{Hello time}$  (default: 3 times 2 seconds) or within a few milliseconds of a physical link failure. The so-called Hello time is an important and configurable time interval that is used by RSTP for several purposes; its default value is 2 seconds.<sup>[8][9]</sup>

Standard IEEE 802.1D-2004 incorporates RSTP and obsoletes the original STP standard.<sup>[10]</sup>

## Rapid Spanning Tree Operation

RSTP adds new bridge port roles in order to speed convergence following a link failure.

### RSTP bridge port roles:

- **Root** - A forwarding port that is the best port from Nonroot-bridge to Rootbridge
- **Designated** - A forwarding port for every LAN segment
- **Alternate** - An alternate path to the root bridge. This path is different than using the root port.
- **Backup** - A backup/redundant path to a segment where another bridge port already connects.
- **Disabled** - Not strictly part of STP, a network administrator can manually disable a port

Additional RSTP Operation Details:

- Detection of root switch failure is done in 3 hello times, which is 6 seconds if default hello times have not been changed.
- Ports may be configured as edge ports if they are attached to a LAN that has no other bridges attached. These edge ports transition directly to the forwarding state. RSTP still continues to monitor the port for BPDUs in case a bridge is connected. RSTP can also be configured to automatically detect edge ports. As soon as the bridge detects a BPDU coming to an edge port, the port becomes a non-edge port.
- Unlike in STP, RSTP will respond to BPDUs sent from the direction of the root bridge. An RSTP bridge will "propose" its spanning tree information to its designated ports. If another RSTP bridge receives this information and determines this is the superior root information, it sets all its other ports to discarding. The bridge may send an "agreement" to the first bridge confirming its superior spanning tree information. The first bridge, upon receiving this agreement, knows it can rapidly transition that port to the forwarding state bypassing the traditional listening/learning state transition. This essentially creates a cascading effect away from the root bridge where each designated bridge proposes to its neighbors to determine if it can make a rapid transition. This is one of the major elements that allows RSTP to achieve faster convergence times than STP.
- As discussed in the port role details above, RSTP maintains backup details regarding the discarding status of ports. This avoids timeouts if the current forwarding ports were to fail or BPDUs were not received on the root port in a certain interval.
- RSTP will revert to legacy STP on an interface if a legacy version of an STP BPDU is detected on that port.

## Per-VLAN Spanning Tree and Per-VLAN Spanning Tree Plus

In Ethernet switched environments where multiple Virtual LANs exist, it is often necessary to create multiple spanning trees so that traffic from different VLANs uses different links. Cisco's proprietary versions of Spanning Tree Protocol that allows for the creation of a spanning tree for each VLAN are called *Per-VLAN Spanning Tree* (PVST) and *Per-VLAN Spanning Tree Plus* (PVST+). Both PVST and PVST+ protocols are Cisco proprietary protocols and they cannot be used on most third party switches. Some equipment from Force10 Networks, Extreme Networks, Avaya and Blade Network Technologies support PVST+.<sup>[11][12][13]</sup> Extreme Networks does so with two limitations (lack of support on ports where the VLAN is untagged/native and also on the VLAN with ID 1). PVST works only with ISL (Cisco's proprietary protocol for VLAN encapsulation) due to its embedded Spanning tree ID. This is the default protocol on Cisco switches that support ISL. Due to high penetration of the IEEE 802.1Q VLAN trunking standard and PVST's dependence on ISL, Cisco defined a different PVST+ standard that is compatible with 802.1Q encapsulation. This became the default protocol for Cisco switches when Cisco discontinued and removed ISL support from its switches. PVST+ can tunnel across an MSTP Region.<sup>[14]</sup>

## Rapid Per-VLAN Spanning Tree

This is Cisco's proprietary version of Rapid Spanning Tree Protocol. It creates a spanning tree for each VLAN, just like PVST. Cisco refers to this as Rapid Per-VLAN Spanning Tree (RPVST).

## VLAN Spanning Tree Protocol

In Juniper Networks environment, if compatibility to Cisco's proprietary PVST protocol is required, VLAN Spanning Tree Protocol (VSTP) can be configured. VSTP maintains a separate spanning-tree instance for each VLAN configured in the switch. The VSTP protocol is only supported by the EX and MX Series from Juniper Networks. There are two restrictions to the compatibility of VSTP:

1. VSTP supports only 253 different spanning-tree topologies. If there are more than 253 VLANs, it is recommended to configure RSTP in addition to VSTP, and VLANs beyond 253 will be handled by RSTP.
2. MVRP does not support VSTP. If this protocol is in use, VLAN membership for trunk interfaces must be statically configured[15].

By default, VSTP uses the RSTP protocol as its core spanning-tree protocol, but usage of STP can be forced if the network includes old bridges[16].

For more information about configuring VSTP on Juniper Networks switches, go to the official documentation. Understanding VSTP<sup>[16]</sup>

## Multiple Spanning Tree Protocol

The *Multiple Spanning Tree Protocol* (MSTP), originally defined in IEEE 802.1s and later merged into IEEE 802.1Q-2005, defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" Multiple Spanning Tree Protocol configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

If there is only one Virtual LAN (VLAN) in the network, single (traditional) STP works appropriately. If the network contains more than one VLAN, the logical network configured by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

MSTP allows formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (CST).

MSTP is similar to Cisco Systems' Multiple Instances Spanning Tree Protocol (MISTP), and is an evolution of the Spanning Tree Protocol and the Rapid Spanning Tree Protocol. It was introduced in IEEE 802.1s as an amendment to 802.1Q, 1998 edition. Standard IEEE 802.1Q-2005 now includes MSTP.

Unlike some proprietary per-VLAN spanning tree implementations,<sup>[17]</sup> MSTP includes all of its spanning tree information in a single BPDU format. Not only does this reduce the number of BPDUs required on a LAN to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP (and in effect, classic STP too). MSTP does this by encoding additional region information after the standard RSTP BPDU as well as a number of MSTI messages (from 0 to 64 instances, although in practice many bridges support fewer). Each of these MSTI configuration messages conveys the spanning tree information for each instance. Each instance can be assigned a number of configured VLANs and frames (packets) assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. In order to avoid conveying their entire VLAN to spanning tree mapping in each BPDU, bridges encode an MD5 digest of their VLAN to instance table in the MSTP BPDU. This digest is then used by other MSTP bridges, along with other administratively configured values, to determine if the neighboring bridge is in the same MST region as itself.

MSTP is fully compatible with RSTP bridges, in that an MSTP BPDU can be interpreted by an RSTP bridge as an RSTP BPDU. This not only allows compatibility with RSTP bridges without configuration changes, but also causes

any RSTP bridges outside of an MSTP region to see the region as a single RSTP bridge, regardless of the number of MSTP bridges inside the region itself. In order to further facilitate this view of an MST region as a single RSTP bridge, the MSTP protocol uses a variable known as remaining hops as a time to live counter instead of the message age timer used by RSTP. The message age time is only incremented once when spanning tree information enters an MST region, and therefore RSTP bridges will see a region as only one "hop" in the spanning tree. Ports at the edge of an MST region connected to either an RSTP or STP bridge or an endpoint are known as boundary ports. As in RSTP, these ports can be configured as edge ports to facilitate rapid changes to the forwarding state when connected to endpoints.

## Shortest Path Bridging

The IEEE approved the IEEE 802.1aq standard May 2012,<sup>[18]</sup> also known and documented in most books as Shortest Path Bridging (SPB). SPB allows all links to be active through multiple equal cost paths, and provides much larger layer 2 topologies, faster convergence, and improves the use of the mesh topologies through increase bandwidth between all devices by allowing traffic to load share across all paths on a mesh network.<sup>[19][20]</sup> SPB consolidates multiple existing functionalities, including Spanning Tree Protocol (STP), Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), and Multiple MAC Registration Protocol (MMRP) into a one link state protocol.<sup>[21]</sup> SPB is designed to virtually eliminate human error during configuration and preserves the plug-and-play nature that established Ethernet as the de facto protocol at Layer 2.<sup>[21]</sup>

## References

- [1] Perlman, Radia (1985). "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN". *ACM SIGCOMM Computer Communication Review* **15** (4): 44–53. doi:10.1145/318951.319004.
- [2] Perlman, Radia (2000). *Interconnections, Second Edition*. USA: Addison-Wesley. ISBN 0-201-63448-1.
- [3] "802.1D IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges" (<http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>). IEEE. 2004, p. 154. . Retrieved 19 April 2012.
- [4] LAN/MAN Standards Committee of the IEEE Computer Society, ed. (1990). *ANSI/IEEE Std 802.1D*. IEEE
- [5] LAN/MAN Standards Committee of the IEEE Computer Society, ed. (1998). *ANSI/IEEE Std 802.1D, 1998 Edition, Part 3: Media Access Control (MAC) Bridges*. IEEE
- [6] LAN/MAN Standards Committee of the IEEE Computer Society, ed. (2004). *ANSI/IEEE Std 802.1D - 2004: IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*. IEEE
- [7] (PDF) *Understanding Issues Related to Inter-VLAN Bridging* ([http://www.cisco.com/warp/public/473/inter-vlan\\_11072.pdf](http://www.cisco.com/warp/public/473/inter-vlan_11072.pdf)). Cisco Systems, Inc.. 11072.
- [8] Waldemar Wojdak (March 2003 [CPCI203]). "Rapid Spanning Tree Protocol: A new solution from an old technology" (<http://www.compactpci-systems.com/articles/id/?203>). . Retrieved 2008-08-04.
- [9] "Understanding Rapid Spanning Tree Protocol (802.1w)" ([http://www.cisco.com/en/US/tech/tk389/tk621/technologies\\_white\\_paper09186a0080094cfa.shtml](http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml)). . Retrieved 2008-11-27.
- [10] *IEEE 802.1D-2004*, IEEE, 2004-06-04, "Since the original Spanning Tree Protocol (STP) has been removed from the 2004 revision of IEEE Std 802.1D, an implementation of RSTP is required for any claim of conformance for an implementation of IEEE Std 802.1Q-2003 that refers to the current revision of IEEE Std 802.1D"
- [11] "Technical Documentation" ([https://www.force10networks.com/CSPortal20/TechTips/0050B\\_HowDoIConfigureSpanningTree.aspx](https://www.force10networks.com/CSPortal20/TechTips/0050B_HowDoIConfigureSpanningTree.aspx)). Force10Networks. . Retrieved 2011-01-25.
- [12] "ExtremeXOS Operating System, Version 12.5" ([http://www.extremenetworks.com/libraries/products/DSExtXOS\\_1030.pdf](http://www.extremenetworks.com/libraries/products/DSExtXOS_1030.pdf)) (PDF). Extreme Networks. 2010. . Retrieved 2011-01-25.
- [13] "BLADE PVST+ Interoperability with Cisco" ([http://www.bladenetwork.net/userfiles/file/PDFs/WP\\_PVST\\_SpanningTree\\_Cisco.pdf](http://www.bladenetwork.net/userfiles/file/PDFs/WP_PVST_SpanningTree_Cisco.pdf)) (PDF). 2006. . Retrieved 2011-01-25.
- [14] "Bridging Between IEEE 802.1Q VLANs" ([http://www.cisco.com/en/US/docs/ios/12\\_1t/12\\_1t3/feature/guide/dtbridge.html#wp1020686](http://www.cisco.com/en/US/docs/ios/12_1t/12_1t3/feature/guide/dtbridge.html#wp1020686)). Cisco Systems. . Retrieved 2011-01-25.
- [15] [http://www.juniper.net/techpubs/en\\_US/junos10.0/topics/concept/bridging-mvrp-ex-series.html](http://www.juniper.net/techpubs/en_US/junos10.0/topics/concept/bridging-mvrp-ex-series.html)
- [16] [https://www.juniper.net/techpubs/en\\_US/junos9.4/topics/concept/spanning-trees-ex-series-vstp-understanding.html](https://www.juniper.net/techpubs/en_US/junos9.4/topics/concept/spanning-trees-ex-series-vstp-understanding.html)
- [17] "CiscoWorks LAN Management Solution 3.2 Deployment Guide" ([https://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps2425/white\\_paper\\_c07-552114.html#wp9003215](https://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6528/ps2425/white_paper_c07-552114.html#wp9003215)). August 2009. . Retrieved 2010-01-25.
- [18] Shuang Yu (8 May 2012). "IEEE APPROVES NEW IEEE 802.1aq™ SHORTEST PATH BRIDGING STANDARD" (<http://standards.ieee.org/news/2012/802.1aq.html>). IEEE. . Retrieved 2 June 2012.

- [19] Peter Ashwood-Smith (24 Feb 2011). "Shortest Path Bridging IEEE 802.1aq Overview" ([http://meetings.apnic.net/\\_\\_data/assets/pdf\\_file/0012/32007/APRICOT\\_SPB\\_Overview.pdf](http://meetings.apnic.net/__data/assets/pdf_file/0012/32007/APRICOT_SPB_Overview.pdf)). Huawei. . Retrieved 11 May 2012.
- [20] Jim Duffy (11 May 2012). "Largest Illinois healthcare system uproots Cisco to build \$40M private cloud" (<http://www.pcadvisor.co.uk/news/internet/3357242/largest-illinois-healthcare-system-uproots-cisco-build-40m-private-cloud/>). PC Advisor. . Retrieved 11 May 2012. "Shortest Path Bridging will replace Spanning Tree in the Ethernet fabric."
- [21] "IEEE Approves New IEEE 802.1aq Shortest Path Bridging Standard" (<http://www.techpowerup.com/165594/IEEE-Approves-New-IEEE-802.1aq-Shortest-Path-Bridging-Standard.html>). Tech Power Up. 7 May 2012. . Retrieved 11 May 2012.

## External links

- Cisco home page for the Spanning-Tree protocol family ([http://www.cisco.com/en/US/tech/tk389/tk621/tsd\\_technology\\_support\\_protocol\\_home.html](http://www.cisco.com/en/US/tech/tk389/tk621/tsd_technology_support_protocol_home.html)) (discusses CST, MISTP, PVST, PVST+, RSTP, STP)
- STP article in the Wireshark wiki (<http://wiki.wireshark.org/STP>) Includes a sample PCAP-file of captured STP traffic.
- Perlman, Radia. "Algorhyme" (<http://web.archive.org/web/20110719212324/http://www.csua.berkeley.edu/~ranga/humor/algorhyme.txt>). University of California at Berkeley. Archived from the original (<http://www.csua.berkeley.edu/~ranga/humor/algorhyme.txt>) on 2011-07-19. Retrieved 2011-09-01.
- IEEE Standards
  - ANSI/IEEE 802.1D-2004 standard (<http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>), section 17 discusses RSTP (Regular STP is no longer a part of this standard. This is pointed out in section 8.)
  - ANSI/IEEE 802.1Q-2005 standard (<http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf>), section 13 discusses MSTP
- RFCs
  - RFC 2674-1999, proposed standard, Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
  - RFC 1525-1993, - SBRIDGEMIB, proposed standard, Definitions of Managed Objects for Source Routing Bridges
  - RFC 1493-1993 - BRIDGEMIB, draft standard, Definitions of Managed Objects for Bridges
- Spanning Tree Direct vs Indirect Link Failures - CCIE Study (<http://blog.ipexpert.com/2010/03/22/spanning-tree-direct-vs-indirect-link-failures/>)

# IEEE 802.1p

---

**IEEE P802.1p** is the name of a task group active during 1995–98 responsible for adding traffic class expediting and dynamic multicast filtering to the IEEE 802.1D standard. Essentially, they provided a mechanism for implementing Quality of Service (QoS) at the Media Access Control (MAC) level. The group's work with the new priority classes and Generic Attribute Registration Protocol (GARP) was not published separately but was incorporated into a major revision of the standard, IEEE 802.1D-1998. It also required a short amendment extending the frame size of the Ethernet standard by four bytes which was published as **IEEE 802.3ac** in 1998.

The QoS technique developed by the working group, also known as class of service (CoS), is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame header when using VLAN tagged frames as defined by IEEE 802.1Q. It specifies a priority value of between 0 and 7 inclusive that can be used by QoS disciplines to differentiate traffic. Although this technique is commonly referred to as *IEEE 802.1p*, there is no standard or amendment by that name published by the IEEE. Rather the technique is incorporated into IEEE 802.1Q standard which specifies the tag inserted into an Ethernet frame.<sup>[1]</sup>

## Priority levels

Eight different classes of service are available as expressed through the 3-bit PCP field in an IEEE 802.1Q header added to the frame. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE however has made some broad recommendations:<sup>[2]</sup>

PCP	Priority	Acronym	Traffic Types
1	0 (lowest)	BK	Background
0	1	BE	Best Effort
2	2	EE	Excellent Effort
3	3	CA	Critical Applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork Control
7	7 (highest)	NC	Network Control

Note that the above recommendations were revised in IEEE 802.1Q-2005 and differ from the original recommendations found in IEEE 802.1D-2004.

## References

- [1] "IEEE 802.1p: LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization" (<http://www.javvin.com/protocol8021P.html>). Javin. . Retrieved 2012-02-15.
- [2] IEEE 802.1Q-2011, Table I-2 - Traffic type acronyms

# IEEE 802.1Q

**IEEE 802.1Q** is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of **VLAN tagging** for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also contains provisions for a quality of service prioritization scheme commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.

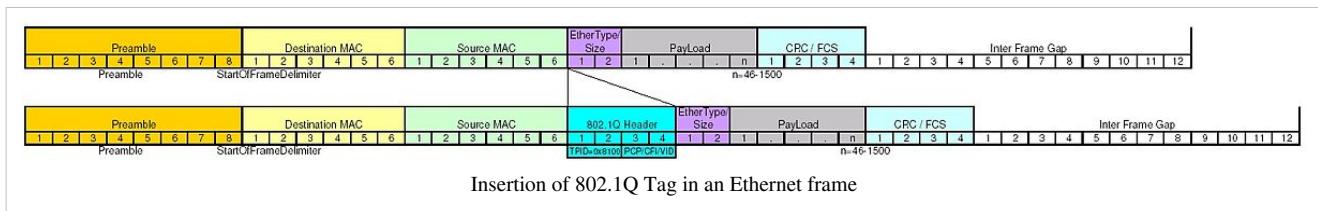
Portions of the network which are *VLAN-aware* (i.e., IEEE 802.1Q conformant) can include VLAN tags. Traffic on a *VLAN-unaware* (i.e., IEEE 802.1D conformant) portion of the network will not contain VLAN tags. When a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership of the frame's port or the port/protocol combination, depending on whether port-based or port-and-protocol-based VLAN classification is being used. Each frame must be distinguishable as being within exactly one VLAN. A frame in the VLAN-aware portion of the network that does not contain a VLAN tag is assumed to be flowing on the native (or default) VLAN.

The standard was developed by IEEE 802.1, a working group of the IEEE 802 standards committee and continues to be actively revised with notable revisions including IEEE 802.1ak, IEEE 802.1Qat and IEEE 802.1Qay.

## Example application

A company wishes to provide data separation and security between network traffic from its various departments by creating separate logical networks for each of its departments dispersed throughout the enterprise, while using only one corporate physical network, which is VLAN-aware. A network administrator assigns a unique VLAN to each department. Edge switches on the corporate network are configured to insert an appropriate VLAN tag into all data frames arriving from equipment belonging to a given department. After the frames are transmitted on their respective VLANs through the corporate network, the VLAN tag is stripped before the frame leaves the VLAN-aware corporate network, and is sent to its destination, which is another computer belonging to the same department.

## Frame format



802.1Q does not actually encapsulate the original frame. Instead, for Ethernet frames, it adds a 32-bit field between the source MAC address and the EtherType/Length fields of the original frame, extending the minimum and maximum frame sizes from 64 and 1,518 bytes (octets) to 64 and 1,522 bytes (42 octet minimum applies when 802.1Q is present. When absent, 46 octet minimum applies. IEEE 802.3-2005 Clause 3.5). Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI). The TCI field is further divided into PCP, CFI, and VID.

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	CFI	VID

- *Tag Protocol Identifier (TPID)*: a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame. This field is located at the same position as the EtherType/Length field in untagged frames, and is thus used to distinguish the frame from untagged frames.
- *Tag Control Identifier (TCI)*
  - *Priority Code Point (PCP)*: a 3-bit field which refers to the IEEE 802.1p priority. It indicates the frame priority level. Values are from 0 (best effort) to 7 (highest); 1 represents the lowest priority. These values can be used to prioritize different classes of traffic (voice, video, data, etc.). *See also Class of Service or CoS*.
  - *Drop Eligible (DE)*: a 1-bit field. May be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion.<sup>[1][2]</sup>
  - *VLAN Identifier (VID)*: a 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 and 0xFFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLANs. The reserved value 0x000 indicates that the frame does not belong to any VLAN; in this case, the 802.1Q tag specifies only a priority and is referred to as a *priority tag*. On bridges, VLAN 1 (the default VLAN ID) is often reserved for a management VLAN; this is vendor-specific.

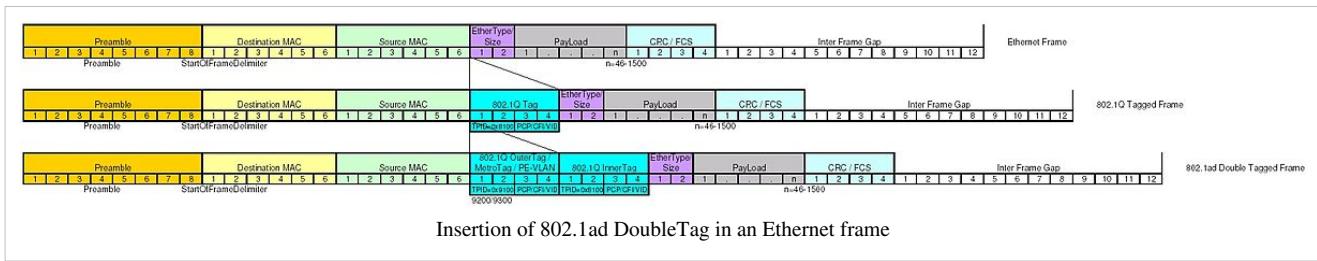
For frames using IEEE 802.2/SNAP encapsulation with an OUI field of 00-00-00 (so that the protocol ID field in the SNAP header is an EtherType), as would be the case on LANs other than Ethernet, the EtherType value in the SNAP header is set to 0x8100 and the aforementioned extra 4 bytes are appended after the SNAP header.

Because inserting the VLAN tag changes the frame, 802.1Q encapsulation forces a recalculation of the original FCS field in the Ethernet trailer.

The 802.1Q standard can create an interesting scenario on the network. Recalling that the maximum size for an Ethernet frame as specified by IEEE 802.3 is 1518 bytes, this means that if a maximum-sized Ethernet frame gets tagged, the frame size will be 1522 bytes, a number that violates the IEEE 802.3 standard. To resolve this issue, the 802.3 committee created a subgroup called 802.3ac to extend the maximum Ethernet size to 1522 bytes. Some network devices that do not support a larger frame size will process the frame successfully but may report these anomalies as a "baby giant."<sup>[3]</sup>

## Double tagging

With the IEEE standard 802.1ad, double-tagging can be useful for Internet service providers, allowing them to use VLANs internally while mixing traffic from clients that are already VLAN-tagged. The outer (next to source MAC and representing ISP VLAN) S-TAG (service tag) comes first, followed by the inner C-TAG (customer tag). In such cases, 802.1ad specifies a TPID of 0x88a8 for service-provider outer S-TAG.



Non-standard triple-tagging is also possible. The third tag of 4 bytes allows extended addressing and also a small hop-count. The 66-bit addressing plan now uses a fixed (non-stacking) QinQinQ format. The result is three 32-bit tags plus the 16-bit EtherType/Length for a total of 112 bits. The two 48-bit (MAC) address fields add another 96

bits. The total header is 208-bits compared to a 320-bit IPv6 header. The 66-bit addressing is 18+48. The 18-bits are encoded 6-bits per 32-bit tag in the 12-bit VID fields. The 16-bit EtherType/Length field can contain the Payload Size or an EtherType for Payloads that contain their own Length, such as IPv4.

<b>16 bits</b>	<b>3 bits</b>	<b>1 bit</b>	<b>12 bits</b>
TPID0	PCP	CFI	VID0
TPID1	CONTENT RATING	CFI	VID1
TPID2	HOP	CFI	VID2

The contents of TPID0+TPID1+TPID2 contain the 48-bit MAC Address of the Source Device.

## Trunk ports and the native VLAN

Clause 9 of the 1998 802.1Q standard defines the encapsulation protocol used to multiplex VLANs over a single link, by adding VLAN tags. However, it is possible to send frames either tagged or untagged, so to help explain which frames will be sent with or without tags, some vendors (most notably Cisco) use the concepts of a) *trunk ports* and b) the *native VLAN* for that trunk.

A trunk port is a port that sends and receives tagged frames on all VLANs, except the native VLAN, if one is configured.

Frames belonging to the native VLAN do NOT carry VLAN tags when sent over the trunk. Conversely, if an untagged frame is received on a trunk port, the frame is associated with the native VLAN configured on that port.

For example, if an 802.1Q port has VLANs 2, 3 and 4 assigned to it, with VLAN 2 being the native VLAN, frames on VLAN 2 that are sent from the aforementioned port are not given an 802.1Q header (i.e. they are plain Ethernet frames). Frames that are received on that port and have no 802.1Q header are assigned to VLAN 2. Tagging of frames sent to or received from VLANs 3 & 4 is the same as if no native VLAN had been configured - all frames on those VLANs must carry tags to identify their VLAN membership.

Note that unexpected results may occur if the native VLAN configuration is not the same on all sending and receiving ports on a link. Continuing the above example, if VLAN 2 is not configured as the native VLAN on some other 802.1Q port, that port will send tagged frames on VLAN 2. When the local port, on which VLAN 2 is configured as the native VLAN, receives these unexpectedly tagged frames, it will still assign them to VLAN 2, but it will send only untagged frames for VLAN 2. On receipt, the distant port will either associate the untagged frames with a different VLAN ID (the one locally configured as the native VLAN) or it will discard the untagged frames if it has no native VLAN configured. (Symmetrically, this remote port will send only untagged frames on its configured native VLAN, which will be associated with a different VLAN ID by the local port.)

Not all vendors use the concept of trunk ports and native VLANs. Annex D to the 1998 802.1Q standard uses the concept of trunk links, but the current (IEEE Std 802.1D- 2004<sup>[3]</sup>) standard does not use the terms *trunk* or *native*. Some use the term "Qtrunk" to avoid confusion with 802.3ad "link aggregation" that is often named a trunk as well.

## Multiple VLAN Registration Protocol

In addition, IEEE 802.1Q defines the Multiple VLAN Registration Protocol (MVRP), an application of the Multiple Registration Protocol, allowing bridges to negotiate the set of VLANs to be used over a specific link.

MVRP replaced the slower GARP VLAN Registration Protocol (GVRP) in 2007 with the IEEE 802.1ak-2007 amendment.

## Multiple Spanning Tree Protocol

The 2003 revision of the standard included the Multiple Spanning Tree Protocol (MSTP) which was originally defined in IEEE 802.1s.

## Notes

- [1] IEEE 802.1Q-2011 clause 6.9.3
- [2] This field was formerly designated *Canonical Format Indicator (CFI)* with a value of 0 indicating a MAC address in canonical format. It is always set to zero for Ethernet. CFI was used for compatibility between Ethernet and Token Ring networks. If a frame received at an Ethernet port had a CFI set to 1, then that frame would not be bridged to an untagged port.
- [3] Understanding Baby Giant/Jumbo Frames Support on Catalyst (<http://www.cisco.com/application/pdf/paws/29805/175.pdf>)

## References

- *IEEE Std. 802.1Q-2005, Virtual Bridged Local Area Networks* (<http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf>). ISBN 0-7381-3662-X.
- *IEEE Std. 802.1Q-2011, Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks* (<http://standards.ieee.org/getieee802/download/802.1Q-2011.pdf>). ISBN 978-0-7381-6708-4.
- ISL & 802.1q Frame Formats ([http://www.cisco.com/en/US/tech/tk389/tk689/technologies\\_tech\\_note09186a0080094665.shtml](http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094665.shtml))

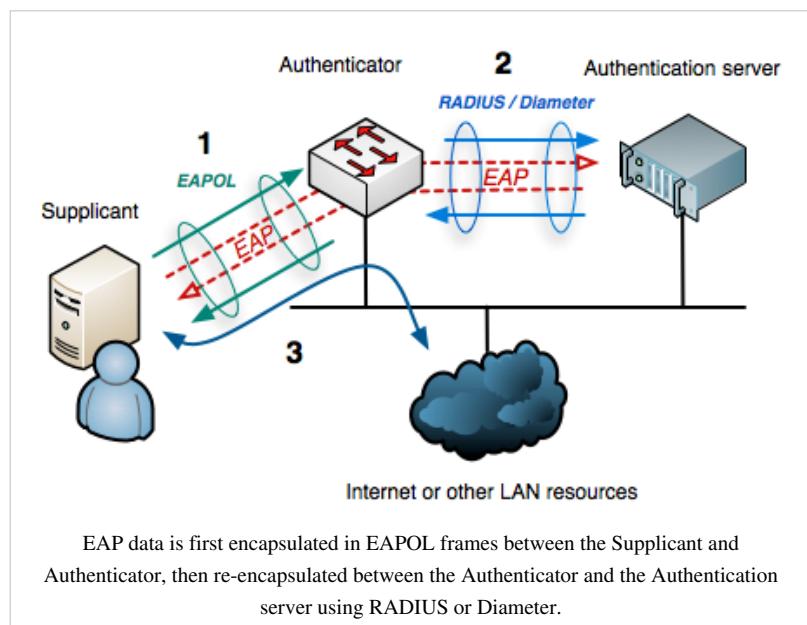
# IEEE 802.1X

**IEEE 802.1X** is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802<sup>[1][2]</sup> which is known as "EAP over LAN" or EAPOL.<sup>[3]</sup> EAPOL was originally designed for IEEE 802.3 Ethernet in 802.1X-2001, but was clarified to suit other IEEE 802 LAN technologies such as IEEE 802.11 wireless and Fiber Distributed Data Interface (ISO 9314-2) in 802.1X-2004.<sup>[4]</sup> The EAPOL protocol was also modified for use with IEEE 802.1AE ("MACsec") and IEEE 802.1AR (Secure Device Identity, DevID) in 802.1X-2010<sup>[5][6]</sup> to support service identification and optional point to point encryption over the local LAN segment.

## Overview

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.



The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name / password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.<sup>[7]</sup>

## Protocol operation

EAPOL operates at the network layer on top of the data link layer, and in Ethernet II framing protocol has an EtherType value of 0x888E.

## Port entities

802.1X-2001 defines two logical port entities for an authenticated port the "controlled port" and the "uncontrolled port". The controlled port is manipulated by the 802.1X PAE (Port Access Entity) to allow (in the authorized state) or prevent (in the unauthorized state) network traffic ingressing and egressing to/from the controlled port. The uncontrolled port is used by the 802.1X PAE to transmit and receive EAPOL frames.

802.1X-2004 defines the equivalent port entities for the supplicant; so a supplicant implementing 802.1X-2004 may prevent higher level protocols being used if it is not content that authentication has successfully completed. This is particularly useful when an EAP method providing Mutual Authentication is used, as the supplicant can prevent data leakage when connected to an unauthorized network.

## Typical authentication progression

1. **Initialization** On detection of a new supplicant, the port on the switch (authenticator) is enabled and set to the "unauthorized" state. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP and HTTP, is dropped.
2. **Initiation** To initiate authentication the authenticator will periodically transmit EAP-Request Identity frames to a special Layer 2 address on the local network segment. The supplicant listens on this address, and on receipt of the EAP-Request Identity frame it responds with an EAP-Response Identity frame containing an identifier for the supplicant such as a User ID. The authenticator then encapsulates this Identity response in a RADIUS Access-Request packet and forwards it on to the authentication server. The supplicant may also initiate or restart authentication by sending an EAPOL-Start frame to the authenticator, which will then reply with an EAP-Request Identity frame.
3. **Negotiation** (*Technically EAP negotiation*) The authentication server sends a reply (encapsulated in a RADIUS Access-Challenge packet) to the authenticator, containing an EAP Request specifying the EAP Method (The type of EAP based authentication it wishes the supplicant to perform). The authenticator encapsulates the EAP Request in an EAPOL frame and transmits it to the supplicant. At this point the supplicant can start using the requested EAP Method, or do an NAK ("Negative Acknowledgement") and respond with the EAP Methods it is willing to perform.
4. **Authentication** If the authentication server and supplicant agree on an EAP Method, EAP Requests and Responses are sent between the supplicant and the authentication server (translated by the authenticator) until the authentication server responds with either an EAP-Success message (encapsulated in a RADIUS Access-Accept packet), or an EAP-Failure message (encapsulated in a RADIUS Access-Reject packet). If authentication is successful, the authenticator sets the port to the "authorized" state and normal traffic is allowed, if it is unsuccessful the port remains in the "unauthorized" state. When the supplicant logs off, it sends an EAPOL-logoff message to the authenticator, the authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic.

## Implementations

### Suplicants

Windows XP, Windows Vista, and Windows 7 support 802.1X for all network connections by default. Windows 2000 has support in the latest service pack (SP4) for wired connections. Windows Mobile 2003 and later operating systems also come with a native 802.1X client.

An open source project known as Open1X produces a client, Xsuplicant. This client currently is available for both Linux and Windows. The main drawbacks of the Open1X client are that it does not provide comprehensible and extensive user documentation and the fact that most Linux vendors do not provide a package for it. The more general wpa\_supplicant can be used for 802.11 wireless networks and wired networks. Both support a very wide range of EAP types.<sup>[8]</sup>

Mac OS X has offered native support since 10.3. The iPhone and iPod Touch support 802.1X as of the release of iOS 2.0.<sup>[9]</sup>

Avenda Systems provides a supplicant for Windows, Linux, and Mac OS X. They also have a plugin for the Microsoft NAP framework.<sup>[10]</sup> Avenda also offers health checking agents as well.

### Windows

Windows defaults to not responding to 802.1X authentication requests for 20 minutes after a failed authentication. This can cause significant disruption to clients. The block period can be configured using the BlockTime value in the registry. A hotfix is required for Windows XP SP3 and Windows Vista SP2 to make the period configurable.<sup>[11]</sup>

Wildcard server certificates are not supported by EAPHost, the Windows component that provides EAP support in the operating system.<sup>[12]</sup> The implication of this is that when using a commercial certification authority, individual certificates must be purchased.

### Windows XP

Windows XP has major issues with its handling of IP address changes that result from user-based 802.1X authentication that changes the VLAN and thus subnet of clients.<sup>[13]</sup> Microsoft has stated that it will not back port the SSO feature from Vista that resolves these issues.<sup>[14]</sup>

If users are not logging in with roaming profiles, a hotfix must be downloaded and installed if authenticating via PEAP with PEAP-MSCHAPv2.<sup>[15]</sup>

### Windows Vista

Windows Vista based computers that are connected via an IP phone may not authenticate as expected and, as a result, the client can be placed in to the wrong VLAN. A hotfix is available to correct this.<sup>[16]</sup>

### Windows 7

Windows 7 based computers that are connected via an IP phone may not authenticate as expected and, as a result, the client can be placed in to the wrong VLAN. A hotfix is available to correct this.<sup>[16]</sup>

Windows 7 does not respond to 802.1X authentication requests after initial 802.1X authentication fails. This can cause significant disruption to clients. A hotfix is available to correct this.<sup>[17]</sup>

## Windows PE

For most enterprises deploying and rolling out operating systems remotely it is worth noting that Windows PE does not natively have any support for 802.1X. However, support can be added to WinPE 2.1<sup>[18]</sup> and WinPE 3.0<sup>[19]</sup> through hotfixes that are available from Microsoft. Although full documentation is not yet available, preliminary documentation for the use of these hotfixes is available via a Microsoft blog.<sup>[20]</sup>

## Federations

eduroam (the international roaming service), mandates the use of 802.1X authentication when providing network access to guests visiting from other eduroam enabled institutions.<sup>[21]</sup>

BT (British Telecom, PLC) employs Identity Federation for authentication in services delivered to a wide variety of industries and governments.<sup>[22]</sup>

## Vulnerabilities in 802.1X-2001 and 802.1X-2004

### Shared media

In the summer of 2005, Microsoft's Steve Riley posted an article detailing a serious vulnerability in the 802.1X protocol, involving a man in the middle attack. In summary, the flaw stems from the fact that 802.1X authenticates only at the beginning of the connection, but that after authentication, it's possible for an attacker to use the authenticated port if he has the ability to physically insert himself (perhaps using a workgroup hub) between the authenticated computer and the port. Riley suggests that for wired networks the use of IPsec or a combination of IPsec and 802.1X would be more secure.<sup>[23]</sup>

EAPOL-Logoff frames transmitted by the 802.1X supplicant are sent in the clear and contain no data derived from the credential exchange that initially authenticated the client.<sup>[24]</sup> They are therefore trivially easy to spoof on shared media, and can be used as part of a targeted DoS on both wired and wireless LANs. In an EAPOL-Logoff attack a malicious third party with access to the medium the authenticator is attached to, repeatedly sends forged EAPOL-Logoff frames from the target device's MAC Address. The authenticator (believing that the targeted device wishes to end its authentication session) closes the target's authentication session, blocking traffic ingressing from the target, denying it access to the network.

The 802.1X-2010 specification, which began as 802.1af, addresses vulnerabilities in previous 802.1X specifications, by using MACSec IEEE 802.1AE to encrypt data between logical ports (running on top of a physical port) and IEEE 802.1AR (Secure Device Identity / DevID) authenticated devices.<sup>[5][6][25][26]</sup>

As a stopgap until these enhancements are widely implemented, some vendors have extended the 802.1X-2001 and 802.1X-2004 protocol, allowing multiple concurrent authentication sessions to occur on a single port. Whilst this prevents traffic from devices with unauthenticated MAC-Addresses ingressing on an 802.1X authenticated port, it will not stop a malicious device snooping on traffic from an authenticated device and provides no protection against MAC spoofing, or EAPOL-Logoff attacks.

## References

- [1] RFC 3748, § 3.3
- [2] RFC 3748, § 7.12
- [3] IEEE 802.1X-2001, § 7
- [4] IEEE 802.1X-2004, § 3.2.2
- [5] IEEE 802.1X-2010, page iv
- [6] IEEE 802.1X-2010, § 5
- [7] "802.1X Port-Based Authentication Concepts" ([http://www.wireless-nets.com/resources/downloads/802.1x\\_C2.html](http://www.wireless-nets.com/resources/downloads/802.1x_C2.html)). . Retrieved 2008-07-30.
- [8] "eap\_testing.txt from wpa\_supplicant" ([http://hostap.epitest.fi/cgi-bin/viewcvs.cgi/\\*checkout\\*/hostap/wpa\\_supplicant/eap\\_testing.txt](http://hostap.epitest.fi/cgi-bin/viewcvs.cgi/*checkout*/hostap/wpa_supplicant/eap_testing.txt)). . Retrieved 2010-02-10.
- [9] "Apple — iPhone — Enterprise" (<http://www.apple.com/iphone/enterprise/>). . Retrieved 2008-07-31.
- [10] "NAP clients for Linux and Macintosh are available" (<http://blogs.technet.com/b/nap/archive/2008/12/16/nap-clients-for-linux-and-macintosh-are-available.aspx>). 2008-12-16. .
- [11] "A Windows XP-based, Windows Vista-based, or Windows Server 2008-based computer does not respond to 802.1X authentication requests for 20 minutes after a failed authentication" (<http://support.microsoft.com/kb/957931>). Support.microsoft.com. 2009-09-17. . Retrieved 2010-03-23.
- [12] "EAPHost in Windows Vista and Longhorn (January 18, 2006)" (<http://technet.microsoft.com/en-gb/cc730460.aspx>). Technet.microsoft.com. 2007-01-18. . Retrieved 2010-03-24.
- [13] "Problems when obtaining Group Policy objects, roaming profiles, and logon scripts from a Windows Server 2003-based domain controller" (<http://support.microsoft.com/?kbid=935638>). Support.microsoft.com. 2007-09-14. . Retrieved 2010-02-10.
- [14] "802.1X with dynamic VLAN switching — Problems with Roaming Profiles" (<http://forums.technet.microsoft.com/en-US/winserverNAP/thread/f68dc3f0-744a-4d0f-b85a-87f8bc531fd0/>). Forums.technet.microsoft.com. . Retrieved 2010-02-10.
- [15] "A Windows XP Service Pack 3-based client computer cannot use the IEEE 802.1X authentication when you use PEAP with PEAP-MSCHAPv2 in a domain" (<http://support.microsoft.com/kb/969111>). Support.microsoft.com. 2009-04-23. . Retrieved 2010-03-23.
- [16] "A computer that is connected to an IEEE 802.1X authenticated network through a VOIP phone does not connect to the correct network after you resume it from Hibernate mode or Sleep mode" (<http://support.microsoft.com/kb/976373>). Support.microsoft.com. 2010-02-08. . Retrieved 2010-03-23.
- [17] "Windows 7 or Windows Server 2008 R2 does not respond to 802.1X authentication requests after the authentication fails" (<http://support.microsoft.com/kb/980295>). Support.microsoft.com. 2010-03-08. . Retrieved 2010-03-23.
- [18] "Windows PE 2.1 does not support the IEEE 802.1X authentication protocol" (<http://support.microsoft.com/kb/975483>). Support.microsoft.com. 2009-12-08. . Retrieved 2010-02-10.
- [19] "The IEEE 802.1X authentication protocol is not supported in Windows Preinstall Environment (PE) 3.0" (<http://support.microsoft.com/kb/972831>). Support.microsoft.com. 2009-12-08. . Retrieved 2010-02-10.
- [20] "Adding Support for 802.1X to WinPE" (<http://blogs.technet.com/deploymentguys/archive/2010/03/02/adding-support-for-802-1x-to-winpe.aspx>). Blogs.technet.com. 2010-03-02. . Retrieved 2010-03-03.
- [21] "Eduroam — About" (<http://www.eduroam.org/index.php?p=about>). . Retrieved 2009-11-29.
- [22] "BT Identity and Access Management" ([http://www.ca.com/files/SuccessStories/bt\\_ss\\_165270.pdf](http://www.ca.com/files/SuccessStories/bt_ss_165270.pdf)). . Retrieved 2010-08-17.
- [23] "Steve Riley's article on the 802.1X vulnerabilities" (<http://www.microsoft.com/technet/community/columns/secmgmt/sm0805.mspx>). Microsoft.com. 2005-08-09. . Retrieved 2010-02-10.
- [24] IEEE 802.1X-2001, § 7.1
- [25] "2 February 2010 Early Consideration Approvals" (<http://standards.ieee.org/board/rev/110early.html>). Standards.ieee.org. . Retrieved 2010-02-10.
- [26] "IEEE 802.1: 802.1X-2010 - Revision of 802.1X-2004" (<http://www.ieee802.org/1/pages/802.1x-2010.html>). Ieee802.org. 2010-01-21. . Retrieved 2010-02-10.

## External links

- IEEE page on 802.1X (<http://www.ieee802.org/1/pages/802.1x-2004.html>)
- GetIEEE802 Download 802.1X-2010 (<http://standards.ieee.org/getieee802/download/802.1X-2010.pdf>)
- GetIEEE802 Download 802.1X-2004 (<http://standards.ieee.org/getieee802/download/802.1X-2004.pdf>)
- GetIEEE802 Download 802.1X-2001 (<http://standards.ieee.org/getieee802/download/802.1X-2001.pdf>)
- Using 802.1X port authentication to control who can connect to your network ([http://www.itdojo.com/synner/html/synner2/synner2\\_p1.htm](http://www.itdojo.com/synner/html/synner2/synner2_p1.htm))
- Ultimate wireless security guide: Self-signed certificates for your RADIUS server (<http://www.techrepublic.com/article/ultimate-wireless-security-guide-self-signed-certificates-for-your-radius-server/6148560>)
- How to self-sign a RADIUS server for secure 802.1X PEAP or EAP-TTLS authentication (<http://articles.techrepublic.com.com/5100-1035-6148560.html>)
- WIRE1x (<http://wire.cs.nthu.edu.tw/wire1x/>)
- Wired Networking with 802.1X Authentication (<http://technet.microsoft.com/en-us/network/bb545365.aspx>) on Microsoft TechNet

# IEEE 802.3

## Ethernet

**Ethernet** /'i:θərnet/ is a family of computer networking technologies for local area networks (LANs). Ethernet was commercially introduced in 1980 and standardized in 1985 as IEEE 802.3. Ethernet has largely replaced competing wired LAN technologies.

The Ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet. The original 10BASE5 Ethernet used coaxial cable as a shared medium. Later the coaxial cables were replaced by twisted pair and fiber optic links in conjunction with hubs or switches. Data rates were periodically increased from the original 10 megabits per second, to 100 gigabits per second.

Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and re-transmitted. As per the OSI model Ethernet provides services up to and including the data link layer.

Since its commercial release, Ethernet has retained a good degree of compatibility. Features such as the 48-bit MAC address and Ethernet frame format have influenced other networking protocols.



An 8P8C modular connector (often called RJ45) commonly used on cat 5 cables in Ethernet networks

## History

Ethernet was developed at Xerox PARC between 1973 and 1974.<sup>[1][2]</sup> It was inspired by ALOHAnet, which Robert Metcalfe had studied as part of his PhD dissertation.<sup>[3]</sup> The idea was first documented in a memo that Metcalfe wrote on May 22, 1973.<sup>[1][4]</sup> In 1975, Xerox filed a patent application listing Metcalfe, David Boggs, Chuck Thacker and Butler Lampson as inventors.<sup>[5]</sup> In 1976, after the system was deployed at PARC, Metcalfe and Boggs published a seminal paper.<sup>[6][7]</sup>

Metcalfe left Xerox in June 1979 to form 3Com.<sup>[1][8]</sup> He convinced Digital Equipment Corporation (DEC), Intel, and Xerox to work together to promote Ethernet as a standard. The so-called "DIX" standard, for "Digital/Intel/Xerox" specified 10 Mbit/s Ethernet, with 48-bit destination and source addresses and a global 16-bit Ethertype-type field. It was published on September 30, 1980 as "The Ethernet, A Local Area Network. Data Link Layer and Physical Layer Specifications".<sup>[9]</sup> Version 2 was published in November, 1982<sup>[10]</sup> and defines what has become known as Ethernet II. Formal standardization efforts proceeded at the same time.

Ethernet initially competed with two largely proprietary systems, Token Ring and Token Bus. Because Ethernet was able to adapt to market realities and shift to inexpensive and ubiquitous twisted pair wiring, these proprietary protocols soon found themselves competing in a market inundated by Ethernet products and by the end of the 1980s, Ethernet was clearly the dominant network technology.<sup>[11]</sup> In the process, 3Com became a major company. 3Com shipped its first 10 Mbit/s Ethernet 3C100 transceiver in March 1981, and that year started selling adapters for PDP-11s and VAXes, as well as Multibus-based Intel and Sun Microsystems computers.<sup>[11]:9</sup> This was followed quickly by DEC's Unibus to Ethernet adapter, which DEC sold and used internally to build its own corporate

network, which reached over 10,000 nodes by 1986, making it one of the largest computer networks in the world at that time.<sup>[12]</sup> An Ethernet adapter card for the IBM PC was released in 1982 and by 1985, 3Com had sold 100,000.<sup>[8]</sup>

Since then Ethernet technology has evolved to meet new bandwidth and market requirements.<sup>[13]</sup> In addition to computers, Ethernet is now used to interconnect appliances and other personal devices.<sup>[1]</sup> It is used in industrial applications and is quickly replacing legacy data transmission systems in the world's telecommunications networks.<sup>[14]</sup> By 2010, the market for Ethernet equipment amounted to over \$16 billion per year.<sup>[15]</sup>

## Standardization

In February 1980, the Institute of Electrical and Electronics Engineers (IEEE) started project 802 to standardize local area networks (LAN).<sup>[16][8]</sup> The "DIX-group" with Gary Robinson (DEC), Phil Arst (Intel), and Bob Printis (Xerox) submitted the so-called "Blue Book" CSMA/CD specification as a candidate for the LAN specification.<sup>[9]</sup> In addition to CSMA/CD, Token Ring (supported by IBM) and Token Bus (selected and henceforward supported by General Motors) were also considered as candidates for a LAN standard. Competing proposals and broad interest in the initiative led to strong disagreement over which technology to standardize. In December 1980, the group was split into three subgroups, and standardization proceeded separately for each proposal.<sup>[8]</sup>

Delays in the standards process put at risk the market introduction of the Xerox Star workstation and 3Com's Ethernet LAN products. With such business implications in mind, David Liddle (General Manager, Xerox Office Systems) and Metcalfe (3Com) strongly supported a proposal of Fritz Röscheisen (Siemens Private Networks) for an alliance in the emerging office communication market, including Siemens' support for the international standardization of Ethernet (April 10, 1981). Ingrid Fromm, Siemens' representative to IEEE 802, quickly achieved broader support for Ethernet beyond IEEE by the establishment of a competing Task Group "Local Networks" within the European standards body ECMA TC24. As early as March 1982 ECMA TC24 with its corporate members reached agreement on a standard for CSMA/CD based on the IEEE 802 draft.<sup>[11]:8</sup> Because the DIX proposal was most technically complete and because of the speedy action taken by ECMA which decisively contributed to the conciliation of opinions within IEEE, the IEEE 802.3 CSMA/CD standard was approved in December 1982.<sup>[8]</sup> IEEE published the 802.3 standard as a draft in 1983 and as a standard in 1985.

Approval of Ethernet on the international level was achieved by a similar, cross-partisan action with Fromm as liaison officer working to integrate International Electrotechnical Commission, TC83 and International Organization for Standardization (ISO) TC97SC6, and the ISO/IEEE 802/3 standard was approved in 1984.

## Evolution

Ethernet evolved to include higher bandwidth, improved media access control methods, and different physical media. The coaxial cable was replaced with point-to-point links connected by Ethernet repeaters or switches to reduce installation costs, increase reliability, and improve management and troubleshooting. Many variants of Ethernet remain in common use.

Ethernet stations communicate by sending each other data packets: blocks of data individually sent and delivered. As with other IEEE 802 LANs, each Ethernet station is given a 48-bit MAC address. The MAC addresses are used to specify both the destination and the source of each data packet. Ethernet establishes link level connections, which can be defined using both the destination and source addresses. On reception of a transmission, the receiver uses the destination address to determine whether the transmission is relevant to the station or should be ignored. Network interfaces normally do not accept packets addressed to other Ethernet stations. Adapters come programmed with a globally unique address.<sup>[17]</sup> An Ethertype field in each frame is used by the operating system on the receiving station to select the appropriate protocol module (i.e. the Internet protocol module). Ethernet frames are said to be *self-identifying*, because of the frame type. Self-identifying frames make it possible to intermix multiple protocols on the same physical network and allow a single computer to use multiple protocols together.<sup>[18]</sup> Despite the evolution

of Ethernet technology, all generations of Ethernet (excluding early experimental versions) use the same frame formats<sup>[19]</sup> (and hence the same interface for higher layers), and can be readily interconnected through bridging.

Due to the ubiquity of Ethernet, the ever-decreasing cost of the hardware needed to support it, and the reduced panel space needed by twisted pair Ethernet, most manufacturers now build Ethernet interfaces directly into PC motherboards, eliminating the need for installation of a separate network card.<sup>[20]</sup>

## Shared media

Ethernet was originally based on the idea of computers communicating over a shared coaxial cable acting as a broadcast transmission medium. The methods used were similar to those used in radio systems,<sup>[21]</sup> with the common cable providing the communication channel likened to the *Luminiferous aether* in 19th century physics, and it was from this reference that the name "Ethernet" was derived.<sup>[22]</sup>

Original Ethernet's shared coaxial cable (the shared medium) traversed a building or campus to every attached machine. A scheme known as carrier sense multiple access with collision detection (CSMA/CD) governed the way the computers shared the channel. This scheme was simpler than the competing token ring or token bus technologies.<sup>[23]</sup> Computers were connected to an Attachment Unit Interface (AUI) transceiver, which was in turn connected to the cable (later with thin Ethernet the transceiver was integrated into the network adapter).

While a simple passive wire was highly reliable for small networks, it was not reliable for large extended networks, where damage to the wire in a single place, or a single bad connector, could make the whole Ethernet segment unusable.<sup>[24]</sup>

Through the first half of the 1980s, Ethernet's 10BASE5 implementation used a coaxial cable 0.375 inches (**unknown operator: u'strong'** mm) in diameter, later called "thick Ethernet" or "thicknet". Its successor, 10BASE2, called "thin Ethernet" or "thinnet", used a cable similar to cable television cable of the era. The emphasis was on making installation of the cable easier and less costly.

Since all communications happen on the same wire, any information sent by one computer is received by all, even if that information is intended for just one destination.<sup>[25]</sup> The network interface card interrupts the CPU only when applicable packets are received: The card ignores information not addressed to it.<sup>[26]</sup> Use of a single cable also means that the bandwidth is shared, such that, for example, available bandwidth to each device is halved when two stations are simultaneously active.

Collisions corrupt transmitted data and require stations to retransmit. The lost data and retransmissions reduce throughput. In the worst case where multiple active hosts connected with maximum allowed cable length attempt to transmit many short frames, excessive collisions can reduce throughput dramatically. However, a Xerox report in 1980 studied performance of an existing Ethernet installation under both normal and artificially generated heavy load. The report claims that 98% throughput on the LAN was observed.<sup>[27]</sup> This is in contrast with token passing LANs (token ring, token bus), all of which suffer throughput degradation as each new node comes into the LAN, due to token waits. This report was controversial, as modeling showed that collision-based networks became unstable under loads as low as 40% of nominal capacity. Many early researchers failed to understand the subtleties of the CSMA/CD protocol and how important it was to get the details right, and were really modeling somewhat different networks (usually not as good as real Ethernet).<sup>[28]</sup>



10BASE5 Ethernet equipment

## Repeaters and hubs

For signal degradation and timing reasons, coaxial Ethernet segments had a restricted size. Somewhat larger networks could be built by using an Ethernet repeater. Early repeaters had only two ports, allowing, at most, a doubling of network size. Once repeaters with more than two ports became available, it was possible to wire the network in a star topology. Early experiments with star topologies (called "Fibernet") using optical fiber were published by 1978.<sup>[29]</sup>

Shared cable Ethernet was always hard to install in offices because its bus topology was in conflict with the star topology cable plans designed into buildings for telephony. Modifying Ethernet to conform to twisted pair telephone wiring already installed in commercial buildings provided another opportunity to lower costs, expand the installed base, and leverage building design, and, thus, twisted-pair Ethernet was the next logical development in the mid-1980s.



A 1990s network interface card supporting both coaxial cable-based 10BASE2 (BNC connector, left) and twisted pair-based 10BASE-T (8P8C connector, right)

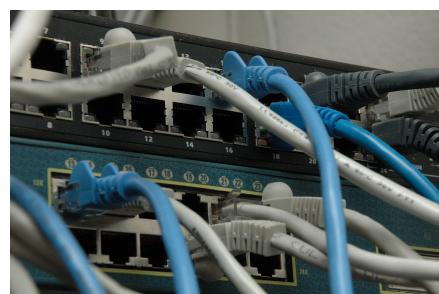
Ethernet on unshielded twisted-pair cables (UTP) began with StarLAN at 1 Mbit/s in the mid-1980s. In 1987 SynOptics introduced the first twisted-pair Ethernet at 10 Mbit/s in a star-wired cabling topology with a central hub, later called LattisNet.<sup>[30][31][8]</sup> These evolved into 10BASE-T, which was designed for point-to-point links only, and all termination was built into the device. This changed repeaters from a specialist device used at the center of large networks to a device that every twisted pair-based network with more than two machines had to use. The tree structure that resulted from this made Ethernet networks easier to maintain by preventing most faults with one peer or its associated cable from affecting other devices on the network.

Despite the physical star topology and the presence of separate transmit and receive channels in the twisted pair and fiber media, repeater based Ethernet networks still use half-duplex and CSMA/CD, with only minimal activity by the repeater, primarily the Collision Enforcement signal, in dealing with packet collisions. Every packet is sent to every port on the repeater, so bandwidth and security problems are not addressed. The total throughput of the repeater is limited to that of a single link, and all links must operate at the same speed.

## Bridging and switching

While repeaters could isolate some aspects of Ethernet segments, such as cable breakages, they still forwarded all traffic to all Ethernet devices. This created practical limits on how many machines could communicate on an Ethernet network. The entire network was one collision domain, and all hosts had to be able to detect collisions anywhere on the network. This limited the number of repeaters between the farthest nodes. Segments joined by repeaters had to all operate at the same speed, making phased-in upgrades impossible.

To alleviate these problems, bridging was created to communicate at the data link layer while isolating the physical layer. With bridging, only well-formed Ethernet packets are forwarded from one Ethernet segment to another; collisions and packet errors are isolated. Prior to learning of network devices on the different segments, Ethernet bridges (and switches) work somewhat like Ethernet repeaters, passing all traffic between segments. After the bridge learns the addresses associated with each port, it forwards network traffic only to the necessary segments, improving overall



Patch cables with patch fields of two Ethernet switches

performance. Broadcast traffic is still forwarded to all network segments. Bridges also overcame the limits on total segments between two hosts and allowed the mixing of speeds, both of which are critical to deployment of Fast Ethernet.

In 1989, the networking company Kalpana introduced their EtherSwitch, the first Ethernet switch.<sup>[32]</sup> This worked somewhat differently from an Ethernet bridge, where only the header of the incoming packet would be examined before it was either dropped or forwarded to another segment. This greatly reduced the forwarding latency and the processing load on the network device. One drawback of this cut-through switching method was that packets that had been corrupted would still be propagated through the network, so a jabbering station could continue to disrupt the entire network. The eventual remedy for this was a return to the original store and forward approach of bridging, where the packet would be read into a buffer on the switch in its entirety, verified against its checksum and then forwarded, but using more powerful application-specific integrated circuits. Hence, the bridging is then done in hardware, allowing packets to be forwarded at full wire speed.

When a twisted pair or fiber link segment is used and neither end is connected to a repeater, full-duplex Ethernet becomes possible over that segment. In full-duplex mode, both devices can transmit and receive to and from each other at the same time, and there is no collision domain. This doubles the aggregate bandwidth of the link and is sometimes advertised as double the link speed (e.g., 200 Mbit/s).<sup>[33]</sup> The elimination of the collision domain for these connections also means that all the link's bandwidth can be used by the two devices on that segment and that segment length is not limited by the need for correct collision detection.

Since packets are typically delivered only to the port they are intended for, traffic on a switched Ethernet is less public than on shared-medium Ethernet. Despite this, switched Ethernet should still be regarded as an insecure network technology, because it is easy to subvert switched Ethernet systems by means such as ARP spoofing and MAC flooding.

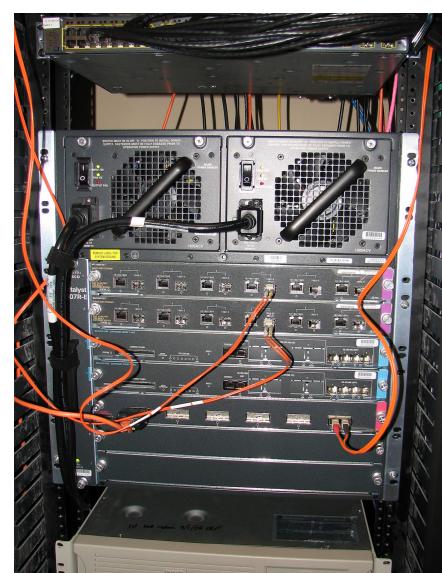
The bandwidth advantages, the slightly better isolation of devices from each other, the ability to easily mix different speeds of devices and the elimination of the chaining limits inherent in non-switched Ethernet have made switched Ethernet the dominant network technology.<sup>[34]</sup>

## Advanced networking

Simple switched Ethernet networks, while a great improvement over repeater-based Ethernet, suffer from single points of failure, attacks that trick switches or hosts into sending data to a machine even if it is not intended for it, scalability and security issues with regard to broadcast radiation and multicast traffic, and bandwidth choke points where a lot of traffic is forced down a single link.

Advanced networking features in switches and routers combat these issues through means including spanning-tree protocol to maintain the active links of the network as a tree while allowing physical loops for redundancy, port security and protection features such as MAC lock down and broadcast radiation filtering, virtual LANs to keep different classes of users separate while using the same physical infrastructure, multilayer switching to route between different classes and link aggregation to add bandwidth to overloaded links and to provide some measure of redundancy.

Networking advances IEEE 802.1aq (SPB) include the use of the link-state routing protocol IS-IS to allow larger networks with shortest path routes between devices.



A core Ethernet switch

## Varieties of Ethernet

The Ethernet physical layer evolved over a considerable time span and encompasses coaxial, twisted pair and fiber optic physical media interfaces and speeds from 10 Mbit to 100 Gbit. The most common forms used are 10BASE-T, 100BASE-TX, and 1000BASE-T. All three utilize twisted pair cables and 8P8C modular connectors. They run at 10 Mbit/s, 100 Mbit/s, and 1 Gbit/s, respectively. Fiber optic variants of Ethernet offer high performance, electrical isolation and distance (tens of kilometers with some versions). In general, network protocol stack software will work similarly on all varieties.

## Ethernet frames

A data packet on the wire is called a frame. A frame begins with preamble and start frame delimiter, followed by an Ethernet header featuring source and destination MAC addresses. The middle section of the frame consists of payload data including any headers for other protocols (e.g., Internet Protocol) carried in the frame. The frame ends with a 32-bit cyclic redundancy check, which is used to detect corruption of data in transit.

## Autonegotiation

Autonegotiation is the procedure by which two connected devices choose common transmission parameters, e.g. speed and duplex mode. Autonegotiation was an optional feature on first introduction of 100BASE-TX, while it is also backward compatible with 10BASE-T. Autonegotiation is mandatory for 1000BASE-T.

## Notes

- [1] *The History of Ethernet* (<http://www.youtube.com/watch?v=g5MezxMcRmk>). NetEvents.tv. 2006. . Retrieved September 10, 2011.
- [2] "Ethernet Prototype Circuit Board" (<http://americanhistory.si.edu/collections/object.cfm?key=35&objkey=96>). Smithsonian National Museum of American History. 1973. . Retrieved September 2, 2007.
- [3] Gerald W. Brock (September 25, 2003). *The Second Information Revolution*. Harvard University Press. p. 151. ISBN 0-674-01178-3.
- [4] Mary Bellis. "Inventors of the Modern Computer" (<http://inventors.about.com/library/weekly/aa111598.htm>). About.com. . Retrieved September 10, 2011.
- [5] U.S. Patent 4063220 (<http://www.google.com/patents?vid=4063220>) "Multipoint data communication system (with collision detection)"
- [6] Robert Metcalfe; David Boggs (July 1976). "Ethernet: Distributed Packet Switching for Local Computer Networks" (<http://www.acm.org/classics/apr96/>). *Communications of the ACM* **19** (7): 395–405. doi:10.1145/360248.360253. .
- [7] The experimental Ethernet described in the 1976 paper ran at 2.94 Mbit/s and had eight-bit destination and source address fields, so the original Ethernet addresses were not the MAC addresses they are today. John F. Shoch; Yogen K. Dalal; David D. Redell; Ronald C. Crane (August 1982). "Evolution of the Ethernet Local Computer Network" (<http://ethernethistory.typepad.com/papers/EthernetEvolution.pdf>). *IEEE Computer* **15** (8): 14–26. doi:10.1109/MC.1982.1654107. . By software convention, the 16 bits after the destination and source address fields specified a "packet type", but, as the paper says, "different protocols use disjoint sets of packet types". Thus the original packet types could vary within each different protocol. This is in contrast to the EtherType in the IEEE Ethernet standard, which specifies the protocol being used.
- [8] Urd Von Burg; Martin Kenny (December 2003). "Sponsors, Communities, and Standards: Ethernet vs. Token Ring in the Local Area Networking Business" ([http://hcd.ucdavis.edu/faculty/webpages/kenney/articles\\_files/Sponsors, Communities, and Standards: Ethernet vs.Token Ring in the Local Area Networking Business.pdf](http://hcd.ucdavis.edu/faculty/webpages/kenney/articles_files/Sponsors, Communities, and Standards: Ethernet vs.Token Ring in the Local Area Networking Business.pdf)). Archived (<http://www.webcitation.org/66LCgXKhx>) from the original on 2012-03-21. .
- [9] Digital Equipment Corporation, Intel Corporation and Xerox Corporation (30 September 1980), *The Ethernet, A Local Area Network. Data Link Layer and Physical Layer Specifications, Version 1.0* (<http://ethernethistory.typepad.com/papers/EthernetSpec.pdf>), Xerox Corporation, , retrieved 2011-12-10
- [10] Digital Equipment Corporation, Intel Corporation and Xerox Corporation (November 1982), *The Ethernet, A Local Area Network. Data Link Layer and Physical Layer Specifications, Version 2.0* (<http://decnet.ipv4.net/docs/dundas/aa-k759b-tk.pdf>), Xerox Corporation, , retrieved 2011-12-10
- [11] Robert Breyer & Sean Riley (1999). *Switched, Fast, and Gigabit Ethernet*. Macmillan. ISBN 1-57870-073-6.
- [12] Jamie Parker Pearson (1992). *Digital at Work*. Digital Press. p. 163. ISBN 1-55558-092-0.
- [13] Rick Merritt (December 20, 2010). *Shifts, growth ahead for 10G Ethernet* (<http://www.eetimes.com/electronics-news/4211609/Shifts-growth-ahead-for-10G-Ethernet>). E Times. . Retrieved September 10, 2011.
- [14] "My oh My – Ethernet Growth Continues to Soar; Surpasses Legacy" (<http://www.jaymiescotto.com/jsablog/2011/07/29/my-oh-my-etherent-growth-continues-to-soar-surpasses-legacy/>). Telecom News Now. July 29, 2011. . Retrieved September 10, 2011.

- [15] Jim Duffy (February 22, 2010). *Cisco, Juniper, HP drive Ethernet switch market in Q4* (<http://www.networkworld.com/news/2010/022210-ethernet-switch-market.html>). Network World. . Retrieved September 10, 2011.
- [16] Vic Hayes (August 27, 2001). "Letter to FCC" (<http://www.ieeeusa.org/policy/policy/2001/01aug27IEEE802.pdf>). . Retrieved October 22, 2010. "IEEE 802 has the basic charter to develop and maintain networking standards... IEEE 802 was formed in February 1980..."
- [17] In some cases, the factory-assigned address can be overridden, either to avoid an address change when an adapter is replaced or to use locally administered addresses.
- [18] Douglas E. Comer (2000). *Internetworking with TCP/IP – Principles, Protocols and Architecture* (4th ed.). Prentice Hall. ISBN 0-13-018380-6. 2.4.9 – Ethernet Hardware Addresses, p. 29, explains the filtering.
- [19] IJitsch van Beijnum. "Speed matters: how Ethernet went from 3Mbps to 100Gbps... and beyond" (<http://arstechnica.com/gadgets/news/2011/07/ethernet-how-does-it-work.ars>). Ars Technica. . Retrieved July 15, 2011. "All aspects of Ethernet were changed: its MAC procedure, the bit encoding, the wiring... only the packet format has remained the same."
- [20] Geetaj Channana (November 1, 2004). "Motherboard Chipsets Roundup" (<http://pcquest.ciol.com/content/search/showarticle.asp?artid=63428>). PCQuest. . Retrieved October 22, 2010. "While comparing motherboards in the last issue we found that all motherboards support Ethernet connection on board."
- [21] There are fundamental differences between wireless and wired shared-medium communications, such as the fact that it is much easier to detect collisions in a wired system than a wireless system.
- [22] Charles E. Spurgeon (2000). *Ethernet: The Definitive Guide*. O'Reilly. ISBN 978-1-56592-660-8.
- [23] In a CSMA/CD system packets must be large enough to guarantee that the leading edge of the propagating wave of the message got to all parts of the medium before the transmitter could stop transmitting, thus guaranteeing that collisions (two or more packets initiated within a window of time that forced them to overlap) would be discovered. Minimum packet size and the physical medium's total length were, thus, closely linked.
- [24] Multipoint systems are also prone to strange failure modes when an electrical discontinuity reflects the signal in such a manner that some nodes would work properly, while others work slowly because of excessive retries or not at all. See standing wave for an explanation. These could be much more difficult to diagnose than a complete failure of the segment.
- [25] This "one speaks, all listen" property is a security weakness of shared-medium Ethernet, since a node on an Ethernet network can eavesdrop on all traffic on the wire if it so chooses.
- [26] Unless it is put into promiscuous mode.
- [27] Shoch, John F. and Hupp, Jon A. (December 1980). "Measured performance of an Ethernet local network" (<http://portal.acm.org/citation.cfm?doid=359038.359044#abstract>). *Communications of the ACM* (ACM Press) **23** (12): 711–721. doi:10.1145/359038.359044. ISSN 0001-0782. .
- [28] Boggs, D.R., Mogul, J.C., and Kent, C.A. (August 1988). "Measured capacity of an Ethernet: myths and reality" (<http://portal.acm.org/citation.cfm?doid=52325.52347#abstract>). *ACM SIGCOMM Computer Communication Review* (ACM Press) **18** (4): 222–234. doi:10.1145/52325.52347. ISBN 0-89791-279-9. .
- [29] Eric G. Rawson; Robert M. Metcalfe (July 1978). "Fibemet: Multimode Optical Fibers for Local Computer Networks" (<http://ethernethistory.typepad.com/papers/Fibernet.pdf>). *IEEE transactions on communications* **26** (7): 983–990. doi:10.1109/TCOM.1978.1094189. . Retrieved June 11, 2011.
- [30] Spurgeon, Charles E. (2000). *Ethernet; The Definitive Guide* ([http://books.google.com/books?id=MRChaUQr0Q0C&pg=PA20&lpg=PA20&dq=synoptics+unshielded+twisted+pair&source=bl&ots=oF5HLbKhsN&sig=aw-dUL9TPoDSaZT0I5ztZvchmjE&hl=en&ei=jGSGTfDQNlqDgAex8InECA&sa=X&oi=book\\_result&ct=result&resnum=1&ved=0CCQQ6AEwADg8#v=onepage&q=synoptics&f=false](http://books.google.com/books?id=MRChaUQr0Q0C&pg=PA20&lpg=PA20&dq=synoptics+unshielded+twisted+pair&source=bl&ots=oF5HLbKhsN&sig=aw-dUL9TPoDSaZT0I5ztZvchmjE&hl=en&ei=jGSGTfDQNlqDgAex8InECA&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCQQ6AEwADg8#v=onepage&q=synoptics&f=false)). Nutshell Handbook, O'Reilly. p. 29. ISBN 1-56592-660-9. .
- [31] Urs von Burg (2001). *The Triumph of Ethernet: technological communities and the battle for the LAN standard* (<http://books.google.com/books?id=ooBqdIXIqbwC&pg=PA175>). Stanford University Press. p. 175. ISBN 0-8047-4094-1. .
- [32] The term *switch* was invented by device manufacturers and does not appear in the 802.3 standard.
- [33] This is misleading, as performance will double only if traffic patterns are symmetrical.
- [34] "Token Ring-to-Ethernet Migration" ([http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns74/ns149/net\\_business\\_benefit09186a00800c92b9\\_ps6600\\_Products\\_White\\_Paper.html](http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns74/ns149/net_business_benefit09186a00800c92b9_ps6600_Products_White_Paper.html)). Cisco. . Retrieved October 22, 2010. "Respondents were first asked about their current and planned desktop LAN attachment standards. The results were clear—switched Fast Ethernet is the dominant choice for desktop connectivity to the network"

## References

### Further reading

- Digital Equipment Corporation, Intel Corporation, Xerox Corporation (September, 1980). *The Ethernet: A Local Area Network* (<http://portal.acm.org/citation.cfm?id=1015591.1015594>). — Version 1.0 of the DIX specification.
- "Internetworking Technology Handbook" ([http://docwiki.cisco.com/wiki/Ethernet\\_Technologies](http://docwiki.cisco.com/wiki/Ethernet_Technologies)). Cisco Systems. Retrieved April 11, 2011.

### External links

- IEEE 802.3 Ethernet working group (<http://www.ieee802.org/3/>)
- IEEE 802.3-2008 standard (<http://standards.ieee.org/getieee802/802.3.html>)

## Link aggregation

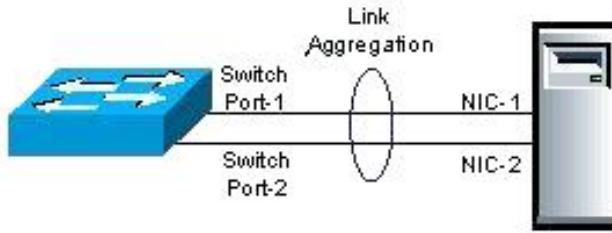
**Link aggregation** is a computer networking term to describe various methods of combining (*aggregating*) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fails.

Further umbrella terms used to describe the method include **port**

**trunking**,<sup>[1]</sup> **link bundling**,<sup>[2]</sup> **Ethernet/network/NIC bonding**,<sup>[1]</sup> or **NIC teaming**. These umbrella terms not only encompass vendor-independent standards such as **IEEE 802.1ax** Link Aggregation Control Protocol (LACP) for wired Ethernet, or the previous **IEEE 802.3ad**, but also various proprietary solutions.

Aggregation can be implemented at any of the lowest three layers of the OSI model. Commonplace examples of aggregation at layer 1 are power line (e.g. IEEE 1901) and wireless (e.g. IEEE 802.11) network devices that combine multiple frequency bands into a single wider one. OSI layer 2 (data link layer, e.g. Ethernet frame in LANs or multi-link PPP in WANs, Ethernet MAC address) aggregation typically occurs across switch ports, which can be either physical ports, or virtual ones managed by an operating system, e.g. such as those of Open vSwitch. Aggregation is also possible at layer 3 in the OSI model, i.e. at the network layer (e.g. IP or IPX), using round-robin scheduling, or based on hash values computed from fields in the packet header, or a combination of these two methods. Regardless of the layer on which aggregation occurs, the network load is balanced across all links. Most methods provide failover/redundancy as well.

Combining can either occur such that multiple interfaces share one logical address (i.e. MAC or IP), or it can be done such that each interface has its own address. The former requires that both ends of a link use the same aggregation method, but has performance advantages over the latter.



Link Aggregation between a switch and a server

## Description

Link aggregation addresses two problems with Ethernet connections: bandwidth limitations and lack of resilience.

With regard to the first issue: bandwidth requirements do not scale linearly. Ethernet bandwidths historically have increased by an order of magnitude each generation: 10 Megabit/s, 100 Mbit/s, 1000 Mbit/s, 10,000 Mbit/s. If one started to bump into bandwidth ceilings, then the only option was to move to the next generation which could be cost prohibitive. An alternative solution, introduced by many of the network manufacturers in the early 1990s, is to combine two physical Ethernet links into one logical link via channel bonding. Most of these solutions required manual configuration and identical equipment on both sides of the aggregation.<sup>[3]</sup>

The second problem involves the three single points of failure in a typical port-cable-port connection. In either the usual computer-to-switch or in a switch-to-switch configuration, the cable itself or either of the ports the cable is plugged into can fail. Multiple physical connections can be made, but many of the higher level protocols were not designed to failover completely seamlessly.

## IEEE Link Aggregation

### Standardization process

By the mid 1990s, most network switch manufacturers had included aggregation capability as a proprietary extension to increase bandwidth between their switches. But each manufacturer developed its own method, which led to compatibility problems. The IEEE 802.3 group took up a study group to create an inter-operable link layer standard in a November 1997 meeting.<sup>[3]</sup> The group quickly agreed to include an automatic configuration feature which would add in redundancy as well. This became known as "Link Aggregation Control Protocol".

### Initial release 802.3ad in 2000

As of 2000 most gigabit channel-bonding schemes use the IEEE standard of Link Aggregation which was formerly clause 43 of the IEEE 802.3 standard added in March 2000 by the IEEE 802.3ad task force.<sup>[4]</sup> Nearly every network equipment manufacturer quickly adopted this joint standard over their proprietary standards.

### Move to 802.1 layer in 2008

David Law noted in 2006 that certain 802.1 layers (such as 802.1X security) were positioned in the protocol stack above Link Aggregation which was defined as an 802.3 sublayer.<sup>[5]</sup> This discrepancy was resolved with formal transfer of the protocol to the 802.1 group with the publication of IEEE 802.1AX-2008 on 3 November 2008.

## Link Aggregation Control Protocol

Within the IEEE specification the **Link Aggregation Control Protocol (LACP)** provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

### Advantages over static configuration

- Failover when a link fails and there is (for example) a Media Converter between the devices which means that the peer will not see the link down. With static link aggregation the peer would continue sending traffic down the link causing it to be lost.
- The device can confirm that the configuration at the other end can handle link aggregation. With Static link aggregation a cabling or configuration mistake could go undetected and cause undesirable network behavior.<sup>[6]</sup>

### Practical notes

LACP works by sending frames (LACPDUs) down all links that have the protocol enabled. If it finds a device on the other end of the link that also has LACP enabled, it will also independently send frames along the same links enabling the two units to detect multiple links between themselves and then combine them into a single logical link. LACP can be configured in one of two modes: active or passive. In active mode it will always send frames along the configured links. In passive mode however, it acts as "speak when spoken to", and therefore can be used as a way of controlling accidental loops (as long as the other device is in active mode).<sup>[4]</sup>

## Proprietary link aggregation

In addition to the IEEE link aggregation substandards, there are a number of proprietary aggregation schemes including Cisco's EtherChannel and Port Aggregation Protocol, Nortel's Multi-link trunking, Split Multi-Link Trunking, Routed Split Multi-Link Trunking and Distributed Split Multi-Link Trunking, ZTE's "Smartgroup", or Huawei's "EtherTrunk". Most high-end network devices support some kind of link aggregation, and software-based implementations – such as the \*BSD *lagg* package, Linux' *bonding* driver, Solaris' *dladm* etc. – also exist for many operating systems.

## Linux Bonding Driver

The linux bonding driver<sup>[7]</sup> provides a method for aggregating multiple network interfaces (nics) into a single logical bonded interface of two or more so called (*nic*) *slaves*. The majority of modern Linux distributions (distros) come with a Linux kernel which has the linux bonding driver integrated as a loadable kernel module and the *ifenslave* (if = (network) interface) user level control program pre-installed. The linux bonding driver was originally programmed by Donald Becker. It came into use with the beowulf cluster patches for the GNU/Linux kernel 2.0.

### Linux Bonding Driver Modes

Modes for the linux bonding driver<sup>[7]</sup> (network interface aggregation modes) are supplied as parameters to the kernel bonding module at load time. They may be given as command line arguments to the insmod or modprobe command, but are usually specified in a linux distribution-specific configuration file. The behavior of the single logical bonded interface depends upon its specified bonding driver mode. The default parameter is balance-rr.

#### Round-robin (balance-rr)

Transmit network packets in sequential order from the first available network interface (nic) slave through the last. This mode provides load balancing and fault tolerance.

#### Active-backup (active-backup)

Only one nic slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. The single logical bonded interface's MAC address is externally visible on only one nic (port) to avoid distortion in the network switch. This mode provides fault tolerance.

#### XOR (balance-xor)

Transmit network packets based on [(source MAC address XOR'd with destination MAC address) modulo nic slave count]. This selects the same nic slave for each destination MAC address. This mode provides load balancing and fault tolerance.

#### Broadcast (broadcast)

Transmit network packets on all slave network interfaces. This mode provides fault tolerance.

#### IEEE 802.3ad Dynamic link aggregation (802.3ad)

Creates aggregation groups that share the same speed and duplex settings. Utilizes all slave network interfaces in the active aggregator group according to the 802.3ad specification.

#### Adaptive transmit load balancing (balance-tlb)

linux bonding driver mode that does not require any special network switch support. The outgoing network packet traffic is distributed according to the current load (computed relative to the speed) on each network interface slave. Incoming traffic is received by one currently designated slave network interface. If this receiving slave fails, another slave takes over the MAC address of the failed receiving slave.

#### Adaptive load balancing (balance-alb)

includes *balance-tlb* plus *receive load balancing* (rlb) for IPV4 traffic, and does not require any special network switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the nic slaves in the single logical bonded interface such that different network-peers use different MAC addresses for their network packet traffic.

## Usage

### Network backbone

Link aggregation offers an inexpensive way to set up a high-speed backbone network that transfers much more data than any one single port or device can deliver. Although, in the past, various vendors used proprietary techniques, the preference today is to use the IEEE standard, which can either be set up statically or by using the Link Aggregation Control Protocol (LACP). This allows several devices to communicate simultaneously at their full single-port speed while not allowing any one single device to monopolize all available backbone capacity.

The actual benefits vary based on the load-balancing method used on each device (administrators can configure different balancing algorithms at each end and this is actually encouraged to avoid path polarization). Link aggregation also allows the network's backbone speed to grow incrementally as demand on the network increases, without having to replace everything and buy new hardware.

Most backbone installations install more cabling or fiber optic pairs than is initially necessary, even if they have no immediate need for the additional cabling. This is done because labor costs are higher than the cost of the cable, and running extra cable reduces future labor costs if networking needs change. Link aggregation can allow the use of these extra cables to increase backbone speeds for little or no extra cost if ports are available.

### Order of frames

When balancing traffic, network administrators often wish to avoid reordering Ethernet frames. For example, TCP suffers additional overhead when dealing with out-of-order packets. This goal is approximated by sending all frames associated with a particular session across the same link.<sup>[8]</sup> The most common implementations use L3 hashes (i.e. based on the IP address), ensuring that the same flow is always sent via the same physical link.

However, depending on the traffic, this may not provide even distribution across the links in the trunk. It effectively limits the client bandwidth in an aggregate to its single member's maximum bandwidth per session. Principally for this reason 50/50 load balancing is almost never reached in real-life implementations; around 70/30 is more usual. Advanced switches can employ an L4 hash (i.e. using TCP/UDP port numbers), which will bring the balance closer to 50/50 as different L4 flows between two hosts can make use of different physical links.

## Efficiency of equipment

Aggregation becomes inefficient beyond a certain bandwidth — depending on the total number of ports on the switch equipment. A 24-port gigabit switch with two 8-gigabit trunks is using sixteen of its available ports just for the two interswitch connections, and leaves only eight of its 1-gigabit ports for other devices. This same configuration on a 48-port gigabit switch leaves 32 1-gigabit ports available, and so it is much more efficient (assuming of course that those ports are actually needed at the switch location).

When a switch utilizes 40-50% of its ports for backbone trunking, upgrading to a switch with either more ports or a higher base-operating speed may be a better option than simply adding more switches, especially if the old switch can be re-used elsewhere on a less performance-critical part of the network.

## Maximum throughput

Multiple switches may be utilized to optimize for maximum throughput in a multiple network switch topology,<sup>[7]</sup> when the switches are configured in parallel as part of an isolated network between two or more systems. In this configuration, the switches are isolated from one another. One reason to employ a topology such as this is for an isolated network with many hosts (a cluster configured for high performance, for example), using multiple smaller switches can be more cost effective than a single larger switch. If access beyond the network is required, an individual host can be equipped with an additional network device connected to an external network; this host then additionally acts as a gateway. The network interfaces 1 through 3 of computer cluster node A, for example, are connected via separate network switches 1 through 3 with network interfaces 1 through 3 of computer cluster node B; there are no inter-connections between the network switches 1 through 3. The linux bonding driver mode typically employed in configurations of this type is balance-rr; the balance-rr mode allows individual connections between two hosts to effectively utilize greater than one interface's bandwidth.

## Use on network interface cards

Network interface cards (NICs) trunked together can also provide network links beyond the throughput of any one single NIC. For example, this allows a central file server to establish an aggregate 2-gigabit connection using two 1-gigabit NICs trunked together. Note the data signaling rate will still be 1Gbit/s, which can be misleading depending on methodologies used to test throughput after link aggregation is employed.

### Microsoft Windows

Microsoft Windows does support native link aggregation starting from Windows Server 2012. For the previous Windows Server versions however, some manufacturers provide software for aggregation on their multiport NICs at the device-driver layer. Intel, for example, has released a package for Windows called Advanced Networking Services (ANS) to bind Intel Fast Ethernet and Gigabit cards.<sup>[9]</sup>

Nvidia also supports "teaming" with their Nvidia Network Access Manager/Firewall Tool. HP also has a teaming tool for HP branded NICs which will allow for non-etherchanneled NIC teaming or which will also support several modes of etherchannel (port aggregation) including 802.3ad with LACP. In addition there is a basic layer-3 aggregation (available at least from Windows XP SP3),<sup>[10]</sup> that allows servers with multiple IP interfaces on the same network to perform load balancing, and home users, with more than 1 internet connection, to increase connection speed by sharing the load on all interfaces.<sup>[11]</sup>

Broadcom offers advanced functions via Broadcom Advanced Control Suite (BACS) via which the teaming-functionality of BASP (advanced server program) are available offering 802.3ad static lags, LACP and "smart teaming" which doesn't require any configuration on the switches to work. It is possible to configure teaming with BACS with a mix of NIC's from different vendors as long as at least one of them is Broadcom and the other NIC's do have the required capabilities to create teaming.<sup>[12]</sup>

## Linux and UNIX

Linux, FreeBSD, NetBSD, OpenBSD, Mac OS X, OpenSolaris and commercial Unix distributions such as AIX implement Ethernet bonding (trunking) at a higher level, and can hence deal with NICs from different manufacturers or drivers, as long as the NIC is supported by the kernel.<sup>[7]</sup>

## Virtualisation platforms

Citrix XenServer and VMware ESX have native support for link-aggregation. XenServer offers both static-LAG's as well as LACP, while ESX(i) only supports static LAG's. With 3<sup>rd</sup> party software based virtual switches it is possible to support LACP under ESX(i): an example of this is the Cisco Nexus 1000v distributed virtual switch<sup>[13]</sup>

For Microsoft's Hyper-V bonding or teaming isn't offered from the hyper-visior or OS-level, but the above mentioned methods for teaming under Windows applies to Hyper-V as well.

## Limitations

### Single switch

With modes balance-rr, balance-xor, broadcast and 802.3ad all physical ports in the link aggregation group must reside on the same logical switch, which in most scenarios will leave a single point of failure when the physical switch to which both links are connected goes offline. Modes active-backup, balance-tlb, and balance-alb can also be set up with two or more switches. But after failover (like all other modes), in some cases, active sessions may fail (due to arp problems) and have to be restarted.

However, almost all vendors have proprietary extensions that resolve some of this issue: they aggregate multiple physical switches into one logical switch. As of 2009, the IEEE has not yet committed resources to standardize this feature. The Split multi-link trunking (SMLT) protocol allows multiple Ethernet links to be split across multiple switches in a stack, preventing any single point of failure, and additionally allowing all switches to be load balanced across multiple aggregation switches from the single access stack. These devices synchronize state across an Inter-Switch Trunk (IST) such that they appear to the connecting (access) device to be a single device (switch block) and prevent any packet duplication. SMLT provides enhanced resiliency with sub-second failover and sub-second recovery for all speed trunks (10 Mbit/s, 100 Mbit/s, 1,000 Mbit/s, and 10 Gbit/s) while operating transparently to end-devices.

### Same link speed

In most implementations, all the ports used in an aggregation consist of the same physical type, such as all copper ports (10/100/1000BASE-T), all multi-mode fiber ports, or all single-mode fiber ports. However, all the IEEE standard requires is that each link be full duplex and all of them have an identical speed (10, 100, 1,000 or 10,000 Mbit/s).

Many switches are PHY independent, meaning that a switch could have a mixture of copper, SX, LX, LX10 or other GBICs. While maintaining the same PHY is the usual approach, it is possible to aggregate a 1000BASE-SX fiber for one link and a 1000BASE-LX (longer, diverse path) for the second link, but the important thing is that the speed will be 1 Gbit/s full duplex for both links. One path may have a slightly longer transit time but the standard has been engineered so this will not cause an issue.

## Ethernet aggregation mismatch

**Aggregation mismatch** refers to not matching the aggregation type on both ends of the link. Some switches do not implement the 802.1AX standard but support static configuration of link aggregation. Therefore link aggregation between similarly statically configured switches will work, but will fail between a statically configured switch and a device that is configured for LACP.

## References

- "Chapter 5.4: Link Aggregation Control Protocol (LACP)" [14]. *IEEE Std 802.1AX-2008 IEEE Standard for Local and Metropolitan Area Networks — Link Aggregation*. IEEE Standards Association. 2008-11-03. p. 30.  
doi:10.1109/IEEESTD.2008.4668665.
  - Tech Tips - Bonding Modes [15]
- [1] Guijarro, Manuel; Ruben Gaspar et al (2008). "Experience and Lessons learnt from running High Availability Databases on Network Attached Storage" ([http://www.iop.org/EJ/article/1742-6596/119/4/042015/jpconf8\\_119\\_042015.pdf](http://www.iop.org/EJ/article/1742-6596/119/4/042015/jpconf8_119_042015.pdf)) (PDF). *Journal of Physics*. Conference Series (IOP Publishing) **119** (4): 042015. doi:10.1088/1742-6596/119/4/042015. . Retrieved 2009-08-17. "Network bonding (also known as port trunking) consists of aggregating multiple network interfaces into a single logical bonded interface that correspond to a single IP address."
- [2] "IEEE 802.3ad Link Bundling" ([http://www.cisco.com/en/US/docs/ios/12\\_2sb/feature/guide/sbcelacp.html](http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/sbcelacp.html)). Cisco Systems. 2007-02-27. . Retrieved 2012-03-15.
- [3] [http://grouper.ieee.org/groups/802/3/trunk\\_study/tutorial/index.html](http://grouper.ieee.org/groups/802/3/trunk_study/tutorial/index.html)
- [4] IEEE 802.3ad Link Aggregation Task Force (<http://www.ieee802.org/3/ad/>)
- [5] Law, David (2006-02-13). "IEEE 802.3 Maintenance" ([http://www.ieee802.org/3/maint/public/maint\\_open\\_1106.pdf](http://www.ieee802.org/3/maint/public/maint_open_1106.pdf)) (PDF). p. 9. . Retrieved 2009-08-18. "Proposal to move Link Aggregation to IEEE 802.1 •It is an 802.3 sublayer but it has to go above IEEE Std 802.1x"
- [6] Link aggregation on Dell servers (<http://support.dell.com/support/edocs/network/LAG1855/LAGConsiderationv0.5.pdf>)
- [7] The Linux Foundation: Bonding (<http://www.linuxfoundation.org/collaborate/workgroups/networking/bonding>)
- [8] [http://grouper.ieee.org/groups/802/3/hssg/public/apr07/frazier\\_01\\_0407.pdf](http://grouper.ieee.org/groups/802/3/hssg/public/apr07/frazier_01_0407.pdf)
- [9] Intel Advanced Networking Services (<http://www.intel.com/support/network/sb/cs-009747.htm>)
- [10] RandomAdapter: Core Services, on MS TechNet ([http://technet.microsoft.com/pl-pl/library/cc784947\(v=ws.10\).aspx](http://technet.microsoft.com/pl-pl/library/cc784947(v=ws.10).aspx))
- [11] Load Balance Network Adapters, at PCTool's Registry Guide for Windows (<http://www.pctools.com/guides/registry/detail/951/>)
- [12] Broadcom Windows Management Applications ([http://www.broadcom.com/support/ethernet\\_nic/management\\_applications.php](http://www.broadcom.com/support/ethernet_nic/management_applications.php)), visited 8 July 2012
- [13] Cisco datasheet Nexus 1000v datasheet ([http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/data\\_sheet\\_c78-492971.html](http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/data_sheet_c78-492971.html)), January, 2012. Visited 8 July 2012
- [14] <http://standards.ieee.org/getieee802/download/802.1AX-2008.pdf>
- [15] <http://techtips.blogfa.com/post-9.aspx>

## External links

- IEEE P802.3ad Link Aggregation Task Force (<http://grouper.ieee.org/groups/802/3/ad/index.html>)
- Mikrotik link Aggregation / Bonding Guide (<http://wiki.mikrotik.com/wiki/Manual:Interface/Bonding>)
- Configuring a Shared Ethernet Adapter ( SEA ) - IBM ([http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/index.jsp?topic=/iphc3\\_p5/iphc3\\_vios\\_configuring\\_sea.htm](http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/index.jsp?topic=/iphc3_p5/iphc3_vios_configuring_sea.htm))
- Managing VLANs on mission-critical shared Ethernet adapters - IBM (<http://www.ibm.com/developerworks/aix/library/au-managevlans/index.html?ca=drs>)

# Power over Ethernet

**Power over Ethernet** or **PoE** technology describes a system to pass electrical power safely, along with data, on Ethernet cabling. The IEEE standard for PoE requires category 5 cable or higher for high power levels, but can operate with category 3 cable if less power is required.<sup>[1]</sup> Power is supplied in common mode over two or more of the differential pairs of wires found in the Ethernet cables and comes from a power supply within a PoE-enabled networking device such as an Ethernet switch or can be *injected* into a cable run with a *midspan* power supply.

The original **IEEE 802.3af-2003**<sup>[2]</sup> PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350 mA<sup>[3][4]</sup>) to each device.<sup>[5]</sup> Only 12.95 W is assured to be available at the powered device as some power is dissipated in the cable.<sup>[6]</sup>

The updated **IEEE 802.3at-2009**<sup>[7]</sup> PoE standard also known as **PoE+** or **PoE plus**, provides up to 25.5 W of power.<sup>[8]</sup> The 2009 standard prohibits a powered device from using all four pairs for power.<sup>[9]</sup> Some vendors have announced products that claim to be compatible with the 802.3at standard and offer up to 51 W of power over a single cable by utilizing all four pairs in the Category 5 cable.<sup>[10]</sup>

Numerous non-standard schemes had been used prior to PoE standardization to provide power over Ethernet cabling. Some are still in active use.



Given a single ethernet cable, a PoE splitter provides both data (gray cable) and power (black cable) for a wireless LAN access point, thus eliminating the need for a nearby power outlet.

## Comparison with other integrated data and power standards

PoE provides both data and power connections in one cable, so equipment doesn't require a separate cable for each need. For equipment that does not already have a power or data connection, PoE can be attractive when the power demand is modest. For example, PoE is useful for IP telephones, wireless LAN access points, cameras with pan tilt and zoom (PTZ), and remote Ethernet switches. PoE can provide long cable runs e.g., 100 meters (**unknown operator: u'strong'** feet) and deliver 12 W of galvanically isolated power. PoE-plus provides even more power.

There are competing technologies. The Universal Serial Bus (USB) provides both data and power, but it is designed for short cables with a maximum length of 5 meters (**unknown operator: u'strong'** feet) and provides less than 2.5 W of non-isolated power. It is less expensive than PoE, and works well for low power peripherals such as a computer mouse, a headset/microphone, or a serial port. Some peripherals, such as speakers, scanners, and printers, need more power than USB can provide. Firewire (IEEE 1394) is similar to USB, but can provide substantially more power (45 W) but has an even shorter limit on cables at 4.5 m. On the other hand, USB peripherals can operate using very little power; while maintaining an Ethernet connection uses a significant amount of power.

If a device already has power available but no data link, then PoE may not be attractive. A wireless data connection such as IEEE 802.11 may be more economical than running a data cable for the device. Alternatively, there are power line communication technologies that can use power cables for transmitting data. Using some power line

modems may be more economical than running a cable.

When data rate and power requirements are both low, other approaches may be viable. Cellular phones, for example, use batteries for power and wireless for data link. Remote weather sensors uses very low data rates, so batteries (possibly supplemented with solar power) and custom wireless data links are used. Replacing batteries is a nuisance, but if the batteries last six months to a year, the practice may be tolerable.

Depending on the application, some of the advantages with PoE over other technologies may be:

- Inexpensive cabling
- Modest power
- Fast data rate
- Peer-to-peer network access. Once a device is connected to the network, it is accessible to many users.

## Uses

Some types of devices with PoE include:<sup>[11]</sup>

- IP Security Cameras
- Network routers
- A mini network switch installed in distant rooms, to support a small cluster of ports from one uplink cable. (These ports on the mini-switch do not themselves provide PoE.) (In most modern VoIP phones a two-port switch is embedded to which a local workstation can be installed using a different VLAN from the voice-VLAN used by the phone itself)
- Network webcams
- Network Intercom / Paging / Public address systems and hallway speaker amplifiers
- VoIP phones
- Wall clocks in rooms and hallways, with time set using Network Time Protocol
- Wireless access points
- Outdoor roof mounted radios with integrated antennas, 802.11 or 802.16 based wireless CPEs (customer premises equipment) used by wireless ISPs.
- Industrial devices (sensors, controllers, meters etc.)
- Access control and Help-points (intercoms, entry cards, keyless entry, etc.)
- Lighting controllers
- Remote Point of Sale (POS) kiosks
- Physical Security devices and controllers



Avaya 1140E IP-Phone with PoE support

## Terminology

### Power sourcing equipment

Power sourcing equipment (PSE) is a device such as a switch that provides ("sources") power on the Ethernet cable. The maximum allowed continuous output power per cable in IEEE 802.3af is 15.40 W. A later specification, IEEE 802.3at, offers 25.50 W.

When the device is a switch, it is commonly called an endspan (although IEEE 802.3af refers to it as endpoint). Otherwise, if it's an intermediary device between a non PoE capable switch and a PoE device, it's called a midspan. An external PoE *injector* is a *midspan* device<sup>[12]</sup>

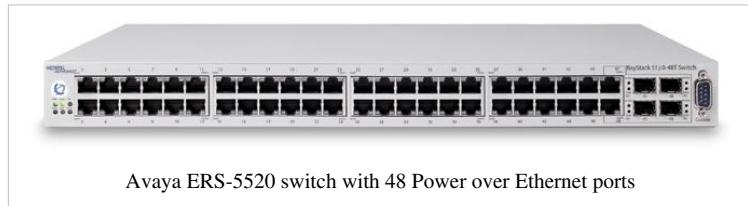
### Powered device

A powered device (PD) is a device powered by a PSE and thus consumes energy. Examples include wireless access points, IP Phones, and IP cameras.

Many powered devices have an auxiliary power connector for an optional, external, power supply. Depending on the PD design, some, none, or all power can be supplied from the auxiliary port,<sup>[13][14]</sup> with the auxiliary port sometimes acting as backup power in case of PoE supplied power failure.

## Power management features and integration

Most advocates expect PoE to become a global longterm DC power cabling standard and replace "wall wart" converters, which cannot be easily centrally managed, waste energy, are often poorly designed, and are easily vulnerable to damage from surges and brownouts.



Avaya ERS-5520 switch with 48 Power over Ethernet ports

Critics of this approach argue that DC power is inherently less efficient than AC power due to the lower voltage, and this is made worse by the thin conductors of Ethernet. A typical 48-port Ethernet switch has a 50 W to 80 W power supply allocated for the traditional Ethernet switch and transceiver IC. Over and above this it requires typically a 370 W (for 802.3af) to 740 W (for 802.3at) power supply allocated solely for PoE ports, permitting a maximum draw on each. This can be quite inefficient to supply through long cables. However, where this central supply replaces several dedicated AC circuits, transformers and inverters, and prevents expensive human interventions (AC installations) the power loss of long thin DC cable is easily justifiable. Power can always be introduced on the device end of the Ethernet cable (radically improving efficiency) where AC power is available.

### Switch power features

Beyond the inherent advantages of an optimized inject-anywhere AC-and-DC cabling infrastructure, the switches themselves often contain "active", "smart", or "managed" power management features to further reduce AC draw of all devices combined.

Multi-protocol teaming standards (G.9960, G.hn, and IEEE P1905) and handoff standards (IEEE 802.21) generally rely on simulating Ethernet features in other media. These standards enable more optimal energy and bandwidth management solutions than would otherwise be possible. For instance, networking on existing AC power lines to an outlet where a PoE router is plugged, making it capable of moving a gigabit per second to every device, with minimal wiring, participating fully in both AC and DC device power demand management. Or, letting a session migrate from a high-power Ethernet switch to a low-power power-over-ethernet wireless routing when the need for bandwidth is low and there is no need for power on the Ethernet cable to be supplied to the device.

By late 2011, managed switches with both powered and unpowered Ethernet ports, from Netgear and others, featured many significant energy management features, some of which are proprietary but are likely to migrate into the eventual standard. For instance, "auto power-down and cable-length detection" allowing lower signal strength to be used.<sup>[15]</sup> Given that such features were available in switches selling for under US\$ 250 (November 2011), power savings alone could justify some users switching to a security, VoIP or wireless AP infrastructure based on power over Ethernet, as they would pay for it very quickly.

Power advantages are a major sales appeal of powered over unpowered Ethernet or unpowered alternatives (such as strictly wireless sensor networks, which must in practice rely on batteries if they draw more than their own solar capacity). Advertising for power-over-Ethernet devices usually cites its "green" features including less packaging and improvements over previous models.

## Integrating EEE and PoE

After integration with the IEEE 802.3az Energy-Efficient Ethernet (EEE) standard, the energy management capabilities of the combined standard are expected to be formidable. Pre-standard integrations of EEE and PoE (such as Marvell's **EPPoE** outlined in a May 2011 white paper [16]) claim to achieve a savings upwards of 3 watts per link, extremely significant across the tens of millions of new links shipped each year. These losses are especially significant as higher power devices come online. Marvell claims that:

"With the evolution of PoE from a fairly low power source (up to 12.95W per port) to one with devices of up to 25.5W, the direct current (DC) power losses over Ethernet cables increased exponentially. Approximately 4.5W/port of power is wasted on a CAT5, CAT5e, CAT6 or CAT6A cable...after 100m... EEE typically saves no more than 1W per link, so addressing the 4.5W per link loss from PoE transmission inefficiency would provide much more incremental savings. New energy-efficient PoE (EPPoE) technology can change increase efficiency to 94% while transmitting over the same 25ohm cable, powering IEEE 802.3at-compliant devices in synchronous 4-pairs. When utilizing synchronous 4-pairs, powered devices are fed using all the available wires. For example, on a 24-port IEEE 802.3at-2009 Type 2 system (delivering 25.5W per port), more than 50W are saved." [16]

## Standard implementation

Standards-based power over Ethernet is implemented following the specifications in IEEE 802.3af-2003 (which was later incorporated as clause 33 into IEEE 802.3-2005) or the 2009 update, IEEE 802.3at. A phantom power technique is used to allow the powered pairs to also carry data. This permits its use not only with 10BASE-T and 100BASE-TX, which use only two of the four pairs in the cable, but also with 1000BASE-T (gigabit Ethernet), which uses all four pairs for data transmission. This is possible because all versions of Ethernet over twisted pair cable specify differential data transmission over each pair with transformer coupling; the DC supply and load connections can be made to the transformer center-taps at each end. Each pair thus operates in common mode as one side of the DC supply, so two pairs are required to complete the circuit. The polarity of the DC supply may be inverted by crossover cables; the powered device must operate with either pair: spare pairs 4–5 and 7–8 or data pairs 1–2 and 3–6. Polarity is required on data pairs, and ambiguously implemented for spare pairs, with the use of a diode bridge.

## Standard PoE parameters and comparison

Property	802.3af (802.3at Type 1)	802.3at Type 2
Power available at PD <sup>[17]</sup>	12.95 W	25.50 W
Maximum power delivered by PSE	15.40 W	34.20 W
Voltage range (at PSE)	44.0–57.0 V <sup>[18]</sup>	50.0–57.0 V <sup>[18]</sup>
Voltage range (at PD)	37.0–57.0 V <sup>[19]</sup>	42.5–57.0 V <sup>[19]</sup>
Maximum current	350 mA <sup>[20]</sup>	600 mA <sup>[20]</sup> per mode
Maximum cable resistance	20 Ω (Category 3)	12.5 Ω (Category 5)
Power management	Three power class levels negotiated at initial connection	Four power class levels negotiated at initial connection or 0.1 W steps negotiated continuously
Derating of maximum cable ambient operating temperature	None	5°C with one mode (two pairs) active
Supported cabling	Category 3 and Category 5 <sup>[1]</sup>	Category 5 <sup>[1][21]</sup>
Supported modes	Mode A (endspan), Mode B (midspan)	Mode A, Mode B

Notes:

- [1] IEEE 802.3at-2009, clause 33.1.1c
- [2] *802.3af-2003*, June 2003
- [3] IEEE 802.3-2005, section 2, table 33-5, item 1
- [4] IEEE 802.3-2005, section 2, table 33-5, item 4
- [5] IEEE 802.3-2005, section 2, table 33-5, item 14
- [6] IEEE 802.3-2005, section 2, clause 33.3.5.2
- [7] *802.3at Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements*, September 11, 2009
- [8] "Amendment to IEEE 802.3 Standard Enhances Power Management and Increases Available Power" ([http://standards.ieee.org/announcements/stdbd\\_approves\\_ieee802.3at.html](http://standards.ieee.org/announcements/stdbd_approves_ieee802.3at.html)). IEEE. . Retrieved 2010-06-24.
- [9] Clause 33.3.1 stating, "PDs that simultaneously require power from both Mode A and Mode B are specifically not allowed by this standard."
- [10] "802.3at-2009 Power over Ethernet (PoE) Plus Standard Ratified" (<http://blog.tmcnet.com/blog/tom-keating/voip/8023at-2009-power-over-ethernet-poe-plus-standard-ratified.asp>). . Retrieved 2010-06-24.
- [11] "Power over Ethernet" (<http://www.garrettcom.co.uk/power-over-ethernet>). *Commercial web page*. GarrettCom. . Retrieved August 6, 2011.
- [12] Cisco Aironet technotes on 1000BASE-T mid-span devices (<http://www.cisco.com/en/US/docs/wireless/technology/poe/technical/reference/Power.html#wp40055>), visited 18 July 2011
- [13] IEEE 802.3-2008, section 2, clause 33.3.5
- [14] IEEE 802.3at-2009, clause 33.3.7
- [15] <http://www.netgear.com/business/products/switches/prosafe-plus-switches/GS108PE.aspx>
- [16] <http://www.marvell.com/switching/assets/Marvell-PoE-An-Energy-Efficient-Alternative.pdf>
- [17] Most switched power supplies within the powered device will lose another 10 to 25% of the available power.
- [18] IEEE 802.3at-2009 Table 33-11
- [19] IEEE 802.3at-2009 Table 33-18
- [20] IEEE 802.3at-2009 Table 33-1
- [21] More stringent cable specification allows assumption of more current carrying capacity and lower resistance (20.0 Ohms for Category 3 versus 12.5 Ohms for Category 5).

## Powering devices

Two modes, A and B, are available. Mode A delivers power on the data pairs of 100BASE-TX or 10BASE-T. Mode B delivers power on the spare pairs. PoE can also be used on 1000BASE-T Ethernet in which case, there are no spare pairs and all power is delivered using the phantom technique.

Mode A has two alternate configurations (MDI and MDI-X), using the same pairs but with different polarities. In mode A, pins 1 and 2 (pair #2 in T568B wiring) form one side of the 48 V DC, and pins 3 and 6 (pair #3 in T568B) form the other side. These are the same two pairs used for data transmission in 10BASE-T and 100BASE-TX, allowing the provision of both power and data over only two pairs in such networks. The free polarity allows PoE to accommodate for crossover cables, patch cables and auto-MDIX.

In mode B, pins 4–5 (pair #1 in both T568A and T568B) form one side of the DC supply and pins 7–8 (pair #4 in both T568A and T568B) provide the return; these are the "spare" pairs in 10BASE-T and 100BASE-TX. Mode B, therefore, requires a 4-pair cable.

The PSE, not the powered device (PD), decides whether power mode A or B shall be used. PDs that implement only Mode A or Mode B are disallowed by the standard.

The PSE can implement mode A or B or both. A PD indicates that it is standards-compliant by placing a 25 kΩ resistor between the powered pairs. If the PSE detects a resistance that is too high or too low (including a short circuit), no power is applied. This protects devices that do not support PoE. An optional "power class" feature allows the PD to indicate its power requirements by changing the sense resistance at higher voltages. To stay powered, the PD must continuously use 5–10 mA for at least 60 ms with no more than 400 ms since last use or else it will be unpowered by the PSE.<sup>[1]</sup>

There are two types of PSEs: endspans and midspans. Endspans are Ethernet switches that include the power over Ethernet transmission circuitry. Endspans are commonly called PoE switches. Midspans are power injectors that stand between a regular Ethernet switch and the powered device, injecting power without affecting the data.

Endspans are normally used on new installations or when the switch has to be replaced for other reasons (such as moving from 10/100 Mbit/s to 1 Gbit/s or adding security protocols), which makes it convenient to add the PoE capability. Midspans are used when there is no desire to replace and configure a new Ethernet switch, and only PoE needs to be added to the network.

### Stages of powering up a PoE link

Stage	Action	Volts specified [V]	
		802.3af	802.3at
Detection	PSE detects if the PD has the correct signature resistance of 19–26.5 kΩ	2.7–10.1	
Classification	PSE detects resistor indicating power range (see below)	14.5–20.5	
Mark 1	Signals PSE is 802.3at capable. PD presents a 0.25–4 mA load.	—	7–10
Class 2	PSE outputs classification voltage again to indicate 802.3at capability	—	14.5–20.5
Mark 2	Signals PSE is 802.3at capable. PD presents a 0.25–4 mA load.	—	7–10
Startup	Startup voltage <sup>[2][3]</sup>	> 42	> 42
Normal operation	Supply power to device <sup>[2][3]</sup>	37–57	42.5–57

IEEE 802.3at capable devices are also referred to as "type 2". An 802.3at PSE may also use layer2 communication to signal 802.3at capability.<sup>[4]</sup>

### Power levels available<sup>[5]</sup>

Class	Usage	Classification current [mA]	Power range [Watt]	Class description
0	Default	0–4	0.44–12.94	Classification unimplemented
1	Optional	9–12	0.44–3.84	Very Low power
2	Optional	17–20	3.84–6.49	Low power
3	Optional	26–30	6.49–12.95	Mid power
4	Valid for 802.3at (Type 2) devices, not allowed for 802.3af devices	36–44	12.95–25.50	High power

Class 4 can only be used by IEEE 802.3at (type 2) devices, requiring valid Class 2 and Mark 2 currents for the power up stages. An 802.3af device presenting a class 4 current is considered non-compliant and, instead, will be treated as a Class 0 device.<sup>[6]</sup>

### Configuration via Ethernet layer 2 LLDP

#### LLDP-MED Advanced Power Management<sup>[7]:8</sup>

TLV Header		MED Header		Extended power via MDI			
Type (7 bits)	Length (9 bits)	TIA OUI (3 octets)	Extended power via MDI subtype (1 octet)	Power type (2 bits)	Power source (2 bits)	Power priority (4 bits)	Power value (2 octets)
127	7	00-12-BB	4	PSE or PD	Normal or Backup conservation	Critical, High, Low	0–102.3 W in 0.1 W steps

The setup phases are as follows:

- PSE (provider) tests PD (consumer) physically using 802.3af phase class 3.
  - PSE powers up PD.
- PD sends to PSE: I'm a PD, max power = X, max power requested = X.
- PSE sends to PD: I'm a PSE, max power allowed = X.
  - PD may now use the amount of power as specified by the PSE.

The rules for this power negotiation are:

- PD shall never request more power than physical 802.3af class
- PD shall never draw more than max power advertised by PSE
- PSE may deny any PD drawing more power than max allowed by PSE
- PSE shall not reduce power allocated to PD, that is in use
- PSE may *request* reduced power, via conservation mode<sup>[7]:10</sup>

## Non-standard implementations

### Cisco

Cisco manufactured WLAN access points and IP phones many years before there was an IEEE standard for delivering PoE. Cisco's original PoE implementation is not software upgradeable to the IEEE 802.3af standard. Cisco's original PoE equipment was capable of delivering up to 10 W per port. The amount of power to be delivered is negotiated between the endpoint and the Cisco switch based on a power value that was added to the Cisco proprietary Cisco Discovery Protocol (CDP). CDP is also responsible for dynamically communicating the Voice VLAN value from the Cisco switch to the Cisco IP Phone.

Under Cisco's pre-standard scheme, the PSE (switch) will send a Fast Link Pulse (FLP) on the transmit pair. The PD (device) connects the transmit line to the receive line via a low pass filter. And thus the PSE gets the FLP in return. And a common mode current between pair 1 and 2 will be provided resulting in 48 V DC<sup>[8]</sup> and 6.3 W<sup>[9]</sup> default of allocated power. The PD has then to provide Ethernet link within 5 seconds to the auto-negotiation mode switch port. A later CDP message with a type-length-value tells the PSE its final power requirement. A discontinued link pulses shuts down power.<sup>[10]</sup>

### PowerDsine

PowerDsine, now a Microsemi brand, have been selling midspan power injectors since 1999 with its proprietary *Power over LAN* solution. Several companies such as Polycom, 3Com, Lucent and Nortel utilize PowerDsine's Power over LAN.<sup>[11]</sup>

### Passive

Numerous devices exist which make use of positive power received on pins 4 and 5 of the Ethernet cable, with negative return on pins 7 and 8. In the common "passive" PoE system the injector does not communicate with the powered device to negotiate its wattage requirements, but merely supplies power. Passive DC to DC injectors also exist which convert a 9 V to 36 V DC input power source to a stabilized 24 V 1 A or 48 V 0.5 A PoE feed with pins +4,5 and -7,8. These DC to DC PoE injectors are used in a variety of different telecom applications.<sup>[12]</sup>

### High Wattage, 56V

Certain types of full-ODU (outdoor unit) high capacity microwave radios make use of high wattage PoE injectors which output 56V and are capable of supplying up to 50 or 60 watts of power. The radios themselves typically utilize between 25 to 40 watts, while the PoE injectors are rated for 50 to 60W to account for line loss on up to 100 meters of cat6/cat6a type shielded cable.

### Power capacity limits

Category 5 cable uses 24 AWG conductors, which can safely carry 360 mA at 50 V according to the latest TIA ruling. The cable has eight conductors (only half of which are used for power) and therefore the absolute maximum power transmitted using direct current is  $50 \text{ V} \times 0.360 \text{ A} \times 2 = 36 \text{ W}$ . Considering the voltage drop after 100 m, a PD would be able to receive 31.6 W. The additional heat generated in the wires by PoE at this current level (4.4 watts per 100 meter cable) limits the total number of cables in a bundle to be 100 cables at 45 °C, according to the TIA. This can be somewhat alleviated by the use of Category 6 cable which uses 23 AWG conductors.

## 802.3af Standards A and B

PINS on Switch	10/100 DC on Spares (mode B)	10/100 Mixed DC & Data (mode A)	1000 (1 Gigabit) DC & Bi-Data (mode B)	1000 (1 Gigabit) DC & Bi-Data (mode A)
Pin 1	Rx +	Rx + DC +	TxRx A +	TxRx A + DC +
Pin 2	Rx -	Rx - DC +	TxRx A -	TxRx A - DC +
Pin 3	Tx +	Tx + DC -	TxRx B +	TxRx B + DC -
Pin 4	DC +	unused	TxRx C + DC +	TxRx C +
Pin 5	DC +	unused	TxRx C - DC +	TxRx C -
Pin 6	Tx -	Tx - DC -	TxRx B -	TxRx B - DC -
Pin 7	DC -	unused	TxRx D + DC -	TxRx D +
Pin 8	DC -	unused	TxRx D - DC -	TxRx D -

## References

- [1] Banish Those "Wall Warts" With Power Over Ethernet (<http://www.elecdesign.com/Articles/Index.cfm?ArticleID=5945&pg=3>)
- [2] IEEE 802.3-2008, section 2, table 33-12
- [3] IEEE 802.3at-2009, table 33-18
- [4] "LTC4278 IEEE 802.3at PD with Synchronous No-Opto Flyback Controller and 12V Aux Support" (<http://cds.linear.com/docs/Datasheet/4278fa.pdf>). . 2010-01-11 cds.linear.com
- [5] IEEE 802.3-2005, section 2, table 33-3
- [6] IEEE 802.3-2008, section 2, clause 33.3.4
- [7] "LLDP / LLDP-MED Proposal for PoE Plus (2006-09-15)" (<http://www.ieee802.org/1/files/public/docs2006/ab-congdon-lldp-med-8023at-0906.pdf>). . 2010-01-10
- [8] "Planning for Cisco IP Telephony > Network Infrastructure Analysis" (<http://www.ciscopress.com/articles/article.asp?p=385336&seqNum=2&rll=1>). . 2010-01-12 ciscopress.com
- [9] "Power over Ethernet on the Cisco Catalyst 6500 Series Switch" ([http://www.conticomp.com/PDF/CAT6500POE\\_ds.pdf](http://www.conticomp.com/PDF/CAT6500POE_ds.pdf)). . 2010-01-12 conticomp.com
- [10] "Understanding the Cisco IP Phone 10/100 Ethernet In-Line Power Detection Algorithm - Cisco Systems" ([http://www.cisco.com/en/US/products/hw/phones/ps379/products\\_tech\\_note09186a00801189b5.shtml](http://www.cisco.com/en/US/products/hw/phones/ps379/products_tech_note09186a00801189b5.shtml)). . 2010-01-12 cisco.com
- [11] PowerDsine Limited - The Power over Ethernet Pioneers ([http://www.poweroverethernet.com/sponsors.php?sponsor\\_id=12](http://www.poweroverethernet.com/sponsors.php?sponsor_id=12))
- [12] "Passive Power over Ethernet equipment, AC-DC and DC-DC" (<http://tyconpower.com/products/POE.htm>). . 2010-02-18 tyconpower.com

## External links

- [ieee802.org](http://standards.ieee.org/getieee802/802.3.html): Download the IEEE 802.3 standards (<http://standards.ieee.org/getieee802/802.3.html>)
- [ieee802.org](http://www.ieee802.org/3/af/): IEEE 802.3af Task Force (<http://www.ieee802.org/3/af/>)
- [ieee802.org](http://www.ieee802.org/3/at/): IEEE 802.3at Task Force (<http://www.ieee802.org/3/at/>)

# Gigabit Ethernet

*GigE redirects here. For the camera protocol, see GigE vision.*

In computer networking, **Gigabit Ethernet (GbE or 1 GigE)** is a term describing various technologies for transmitting Ethernet frames at a rate of a gigabit per second (1,000,000,000 bits per second), as defined by the IEEE 802.3-2008 standard. It came into use beginning in 1999, gradually supplanting Fast Ethernet in wired local networks where it performed considerably faster. The cables and equipment are very similar to previous standards, and by the year 2010, were very common and economical.

Half-duplex gigabit links connected through hubs are allowed by the specification,<sup>[1]</sup> but full-duplex usage with switches is much more common.

## History

The result of research done at Xerox PARC in the early 1970s, Ethernet evolved into a widely implemented physical and link layer protocol. Fast Ethernet increased speed from 10 to 100 megabits per second (Mbit/s). Gigabit Ethernet was the next iteration, increasing the speed to 1000 Mbit/s. The initial standard for gigabit Ethernet was produced by the IEEE in June 1998 as **IEEE 802.3z**, and required optical fiber. 802.3z is commonly referred to as 1000BASE-X, where -X refers to either -CX, -SX, -LX, or (non-standard) -ZX.

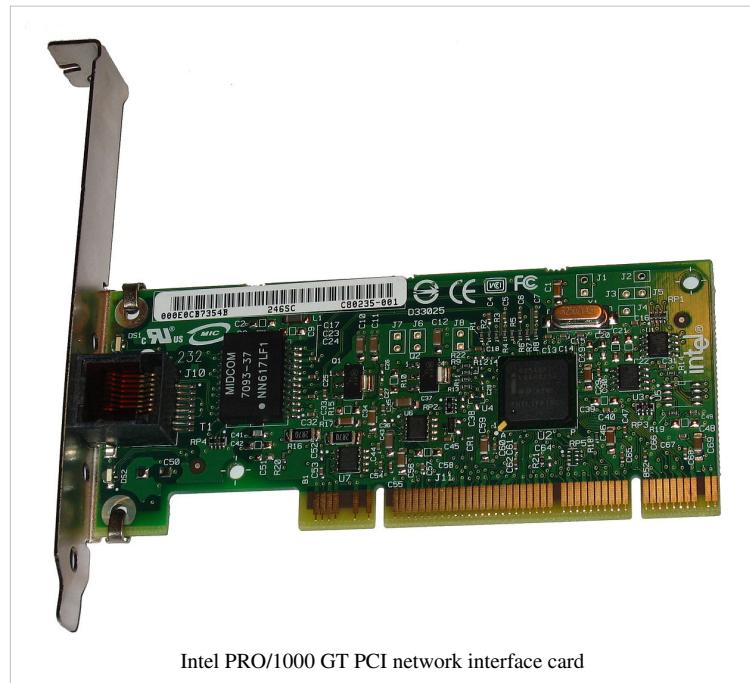
**IEEE 802.3ab**, ratified in 1999, defines gigabit Ethernet transmission over unshielded twisted pair (UTP) category 5,

5e, or 6 cabling and became known as 1000BASE-T. With the ratification of 802.3ab, gigabit Ethernet became a desktop technology as organizations could use their existing copper cabling infrastructure.

**IEEE 802.3ah**, ratified in 2004 added two more gigabit fiber standards, 1000BASE-LX10 (which was already widely implemented as vendor specific extension) and 1000BASE-BX10. This was part of a larger group of protocols known as Ethernet in the First Mile.

Initially, gigabit Ethernet was deployed in high-capacity backbone network links (for instance, on a high-capacity campus network). In 2000, Apple's Power Mac G4 and PowerBook G4 were the first mass produced personal computers featuring the 1000BASE-T connection.<sup>[2]</sup> It quickly became a built-in feature in many other computers.

Higher bandwidth 10 Gigabit Ethernet standards have since become available as the IEEE ratified a fiber-based standard in 2002, and a twisted pair standard in 2006. As of 2009 10Gb Ethernet is replacing 1Gb as the backbone network and has begun to migrate down to high-end server systems.



Intel PRO/1000 GT PCI network interface card

## Varieties

There are five physical layer standards for gigabit Ethernet using optical fiber (1000BASE-X), twisted pair cable (1000BASE-T), or balanced copper cable (1000BASE-CX).

The IEEE 802.3z standard includes 1000BASE-SX for transmission over multi-mode fiber, 1000BASE-LX for transmission over single-mode fiber, and the nearly obsolete 1000BASE-CX for transmission over balanced copper cabling. These standards use 8b/10b encoding, which inflates the line rate by 25%, from 1000 Mbit/s to 1250 Mbit/s, to ensure a DC balanced signal. The symbols are then sent using NRZ.

IEEE 802.3ab, which defines the widely used 1000BASE-T interface type, uses a different encoding scheme in order to keep the symbol rate as low as possible, allowing transmission over twisted pair.

Ethernet in the First Mile later added 1000BASE-LX10 and -BX10.

Name	Medium	Specified distance
1000BASE-CX	Twinaxial cabling	25 meters
1000BASE-SX	Multi-mode fiber	220 to 550 meters dependent on fiber diameter and bandwidth <sup>[3]</sup>
1000BASE-LX	Multi-mode fiber	550 meters <sup>[4]</sup>
1000BASE-LX	Single-mode fiber	5 km <sup>[4]</sup>
1000BASE-LX10	Single-mode fiber using 1,310 nm wavelength	10 km <sup>[4]</sup>
1000BASE-EX	Single-mode fiber at 1,310 nm wavelength	~ 40 km
1000BASE-ZX	Single-mode fiber at 1,550 nm wavelength	~ 70 km
1000BASE-BX10	Single-mode fiber, over single-strand fiber: 1,490 nm downstream 1,310 nm upstream	10 km
1000BASE-T	Twisted-pair cabling (Cat-5, Cat-5e, Cat-6, or Cat-7)	100 meters
1000BASE-TX	Twisted-pair cabling (Cat-6, Cat-7)	100 meters

## 1000BASE-X

1000BASE-X is used in industry to refer to gigabit Ethernet transmission over fiber, where options include 1000BASE-CX, 1000BASE-LX, and 1000BASE-SX, 1000BASE-LX10, 1000BASE-BX10 or the non-standard -ZX implementations.

## 1000BASE-CX

1000BASE-CX is an initial standard for gigabit Ethernet connections over twinaxial cabling with maximum distances of 25 meters using balanced shielded twisted pair and either DE-9 or 8P8C connector. The short segment length is due to very high signal transmission rate. Although it is still used for specific applications where cabling is done by IT professionals, for instance the IBM BladeCenter uses 1000BASE-CX for the Ethernet connections between the blade servers and the switch modules, 1000BASE-T has succeeded it for general copper wiring use.

### **1000BASE-SX**

1000BASE-SX is a fiber optic gigabit Ethernet standard for operation over multi-mode fiber using a 770 to 860 nanometer, near infrared (NIR) light wavelength.

The standard specifies a distance capability between 220 metres (62.5/125 µm fiber with low modal bandwidth) and 550 metres (50/125 µm fiber with high modal bandwidth). In practice, with good quality fiber, optics, and terminations, 1000BASE-SX will usually work over significantly longer distances.

This standard is highly popular for intra-building links in large office buildings, co-location facilities and carrier neutral internet exchanges.

Optical power specifications of SX interface: Minimum output power = -9.5 dBm. Minimum receive sensitivity = -17 dBm.

### **1000BASE-LX**

1000BASE-LX is a fiber optic gigabit Ethernet standard specified in IEEE 802.3 Clause 38 which uses a long wavelength laser (1,270–1,355 nm), and a maximum RMS spectral width of 4 nm.

1000BASE-LX is specified to work over a distance of up to 5 km over 10 µm single-mode fiber.

1000BASE-LX can also run over all common types of multi-mode fiber with a maximum segment length of 550 m. For link distances greater than 300 m, the use of a special launch conditioning patch cord may be required.<sup>[5]</sup> This launches the laser at a precise offset from the center of the fiber which causes it to spread across the diameter of the fiber core, reducing the effect known as differential mode delay which occurs when the laser couples onto only a small number of available modes in multi-mode fiber.

### **1000BASE-LX10**

1000BASE-LX10 was standardized six years after the initial gigabit fiber versions as part of the Ethernet in the First Mile task group. It is very similar to 1000BASE-LX, but achieves longer distances up to 10 km over a pair of single-mode fiber due to higher quality optics. Before it was standardized 1000BASE-LX10 was essentially already in widespread use by many vendors as a proprietary extension called either 1000BASE-LX/LH or 1000BASE-LH.<sup>[6]</sup>

### **1000BASE-EX**

1000BASE-EX is a non-standard but industry accepted term to refer to gigabit Ethernet transmission. It is very similar to 1000BASE-LX10 but achieves longer distances up to 40 km over a pair of single-mode fibers due to higher quality optics than a LX10. Based on the 1,310 nm wavelength and sometimes referred to as LH (Long Haul). Easily confused with a 1000BASE-LX10 or 1000BASE-ZX because some vendors use the LH term.

### **1000BASE-BX10**

1000BASE-BX10 is capable of up to 10 km over a single strand of single-mode fiber, with a different wavelength going in each direction. The terminals on each side of the fibre are not equal, as the one transmitting downstream (from the center of the network to the outside) uses the 1,490 nm wavelength, and the one transmitting upstream uses the 1,310 nm wavelength.

### **1000BASE-ZX**

1000BASE-ZX is a non-standard but industry accepted term to refer to gigabit Ethernet transmission using 1,550 nm wavelength to achieve distances of at least 70 km over single-mode fiber.

## 1000BASE-T

1000BASE-T (also known as IEEE 802.3ab) is a standard for gigabit Ethernet over copper wiring.

Each 1000BASE-T network segment can be a maximum length of 100 meters (328 feet), and must use Category 5 cable or better (including Cat 5e and Cat 6).

Autonegotiation is a requirement for using 1000BASE-T<sup>[7]</sup> according to Section **28D.5 Extensions required for Clause40 (1000BASE-T)**.<sup>[8]</sup> At least the clock source has to be negotiated, as one has to be master and the other slave.

In a departure from both 10BASE-T and 100BASE-TX, 1000BASE-T uses all four cable pairs for simultaneous transmission in both directions through the use of adaptive equalization and a 5-level pulse amplitude modulation (PAM-5) technique. The symbol rate is identical to that of 100BASE-TX (125 Mbaud) and the noise immunity of the 5-level signaling is also identical to that of the 3-level signaling in 100BASE-TX, since 1000BASE-T uses 4-dimensional trellis coded modulation (TCM) to achieve a 6 dB coding gain across the 4 pairs.

Since negotiation takes place on only two pairs, if two gigabit devices are connected through a cable with only two pairs, the devices will successfully choose 'gigabit' as the highest common denominator (HCD), but the link will never come up. Most gigabit physical devices have a specific register to diagnose this behaviour. Some drivers offer an "Ethernet@Wirespeed" option where this situation leads to a slower yet functional connection.<sup>[9]</sup>

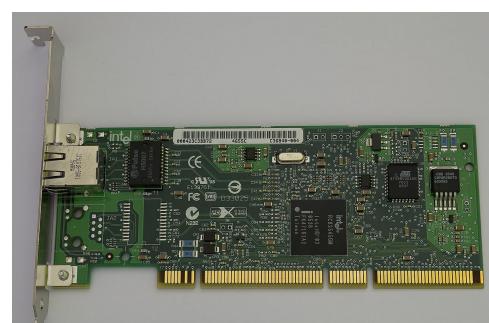
The data is transmitted over four copper pairs, eight bits at a time. First, eight bits of data are expanded into four 3-bit symbols through a non-trivial scrambling procedure based on a linear feedback shift register; this is similar to what is done in 100BASE-T2, but uses different parameters. The 3-bit symbols are then mapped to voltage levels which vary continuously during transmission. An example mapping is as follows:

<b>Symbol</b>	000	001	010	011	100	101	110	111
<b>Line signal level</b>	0	+1	+2	-1	0	+1	-2	-1

*Automatic MDI/MDI-X Configuration* is specified as an optional feature in the 1000BASE-T standard,<sup>[10]</sup> meaning that straight-through cables will often work between gigabit-capable interfaces. This feature eliminates the need for crossover cables, making obsolete the uplink/normal ports and manual selector switches found on many older hubs and switches and greatly reduces installation errors.

## 1000BASE-TX

The Telecommunications Industry Association (TIA) created and promoted a standard similar to 1000BASE-T that was simpler to implement, calling it 1000BASE-TX (TIA/EIA-854).<sup>[11]</sup> The simplified design would, in theory, have reduced the cost of the required electronics by only using one pair of wires in each direction. However, this solution required Category 6 cable and has been a commercial failure, likely due to the cabling requirement as well as the rapidly falling cost of 1000BASE-T products. Many 1000BASE-T products are advertised as 1000BASE-TX due to lack of knowledge that 1000BASE-TX is actually a different standard. The confusion between 1000BASE-T and 1000BASE-TX probably stems from the fact that most popular form of Fast Ethernet (100 Mbit/s) is known as 100BASE-TX, and the fact that many products support multiple speeds of 10/100/1000Mbit/s and are often promoted as 10/100/1000BASE-TX.<sup>[12]</sup>



1000BASE-T capable network interface card made by Intel, which connects to the computer via PCI-X

## Notes

- [1] A single repeater per collision domain is defined in IEEE 802.3 2008 Section 3: 41. Repeater for 1000 Mb/s baseband networks
- [2] "Power Macintosh G4 (Gigabit Ethernet)" (<http://www.apple-history.com/frames/body.php?page=gallery&model=g4giga>). apple-history.com. . Retrieved 2007-11-05.
- [3] IEEE 802.3-2008 Section 3 Table 38-2 p.109
- [4] IEEE 802.3-2008 Section 3 Table 38-6 p.111
- [5] "Mode-Conditioning Patch Cord Installation Note" ([http://www.cisco.com/en/US/products/hw/switches/ps679/products\\_installation\\_and\\_configuration\\_guide09186a008007d1cb.html](http://www.cisco.com/en/US/products/hw/switches/ps679/products_installation_and_configuration_guide09186a008007d1cb.html)). . Retrieved 2009-02-14
- [6] "Cisco SFP Optics For Gigabit Ethernet Applications" ([http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6577/product\\_data\\_sheet0900aecdb8033f885.html](http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6577/product_data_sheet0900aecdb8033f885.html)). Cisco Systems. . Retrieved 2010-06-01.
- [7] "Auto-Negotiation; 802.3-2002" (<http://standards.ieee.org/reading/ieee/interp/IEEE802.3af-2003interp-6.pdf>) (PDF). *IEEE Standards Interpretations*. IEEE. . Retrieved 2007-11-05.
- [8] IEEE. "Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and Physical Layer specifications" ([http://standards.ieee.org/getieee802/download/802.3-2008\\_section2.pdf](http://standards.ieee.org/getieee802/download/802.3-2008_section2.pdf)). SECTION TWO: This section includes Clause21 through Clause 33 and Annex 22A through Annex 33E. . Retrieved 2010-02-18.
- [9] "Broadcom Ethernet NIC FAQs" ([http://www.broadcom.com/support/ethernet\\_nic/faq\\_drivers.php](http://www.broadcom.com/support/ethernet_nic/faq_drivers.php)). . Retrieved 2009-07-25.
- [10] Clause 40.4.4 in IEEE 802.3-2008
- [11] [http://www.tiaonline.org/news\\_events/press\\_room/press\\_releases/legacy.cfm?parelease=01-87](http://www.tiaonline.org/news_events/press_room/press_releases/legacy.cfm?parelease=01-87)
- [12] An example of a product specifying 10/100/1000BASE-TX ports can be found at <http://www.cisco.com/en/US/products/ps10018/index.html>.

## References

### Further reading

- Norris, Mark, *Gigabit Ethernet Technology and Applications*, Artech House, 2002. ISBN 1-58053-505-4

### External links

- Get IEEE 802.3 (<http://standards.ieee.org/getieee802/802.3.html>)
- IEEE 802.3 (<http://www.ieee802.org/3/>)
- IEEE and Gigabit Ethernet Alliance Announce Formal Ratification of gigabit Ethernet Over Copper Standard (<http://standards.ieee.org/announcements/802.3ab.html>) - Announcement from IEEE 28 June 1999
- IEEE P802.3ab 1000BASE-T Task Force (<http://grouper.ieee.org/groups/802/3/ab/>) (historical information)
- IEEE 802.3 CSMA/CD (ETHERNET) (<http://grouper.ieee.org/groups/802/3/>)
- 1000BASE-T Whitepaper from 10GEA (<http://www.10gea.org/1000base-t/>)
- Gigabit Ethernet Auto-Negotiation ([http://www.dell.com/content/topics/global.aspx/power/en/ps1q01\\_hernan?c=us&l=en&cs=555](http://www.dell.com/content/topics/global.aspx/power/en/ps1q01_hernan?c=us&l=en&cs=555))

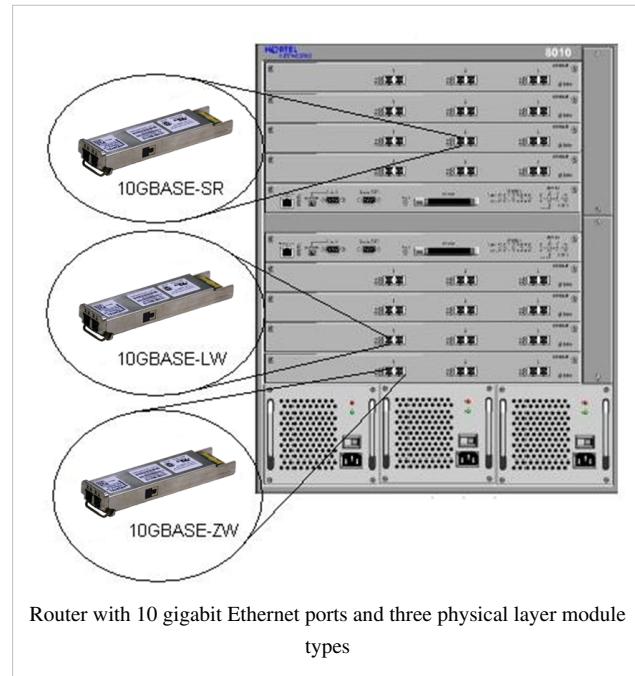
# 10 Gigabit Ethernet

The **10 gigabit Ethernet (10GE or 10GbE or 10 GigE)** computer networking standard was first published in 2002. It defines a version of Ethernet with a nominal data rate of 10 Gbit/s (billion bits per second), ten times faster than gigabit Ethernet. Unlike previous Ethernet standards, 10 gigabit Ethernet defines only full duplex point to point links which are generally connected by network switches. Half duplex operation and hubs do not exist in 10GbE.

The 10 gigabit Ethernet standard encompasses a number of different physical layer (PHY) standards. A networking device may support different PHY types through pluggable PHY modules, such as those based on SFP+. Over time, market forces will determine the most popular 10GE PHY types.<sup>[1]</sup>

At the time that the 10 gigabit Ethernet standard was developed, interest in 10GbE as a wide area network (WAN) transport led to the introduction of a WAN PHY for 10GbE. This operates at a slightly slower data-rate than the local area network (LAN) PHY and adds some extra encapsulation. Both share the same physical medium-dependent sublayers so can use the same optics.

In 2007, one million 10GbE ports were shipped, in 2009 two million ports were shipped, and in 2010 over three million ports were shipped.<sup>[2][3]</sup>



Router with 10 gigabit Ethernet ports and three physical layer module types

## Standards

Over the years the Institute of Electrical and Electronics Engineers (IEEE) 802.3 working group has published several standards relating to 10GbE. These included: 802.3ae-2002 (fiber -SR, -LR, -ER and -LX4 PMDs), 802.3ak-2004 (-CX4 copper twin-ax InfiniBand type cable), 802.3an-2006 (10GBASE-T copper twisted pair), 802.3ap-2007 (copper backplane -KR and -KX4 PMDs) and 802.3aq-2006 (fiber -LRM PMD with enhanced equalization).

The 802.3ae-2002 and 802.3ak-2004 amendments were consolidated into the IEEE 802.3-2005 standard. IEEE 802.3-2005 and the other amendments were consolidated into IEEE Std 802.3-2008.

## Physical layer modules

To support different 10GbE physical layer standards, many interfaces consist of a standard socket into which different PHY modules may be plugged. Physical layer modules are not specified in an official standards body but by multi-source agreements (MSAs) that can be negotiated more quickly. Relevant MSAs for 10GbE include XENPAK (and related X2 and XPAK), XFP and SFP+. When choosing a PHY module, a designer considers cost, reach, media type, power consumption, and size (form factor).



Closeup of an XFP transceiver, in 2008

XENPAK was the first MSA for 10GE and had the largest form factor. X2 and XPAK were later competing standards with smaller form factors. X2 and XPAK have not been as successful in the market as XENPAK. XFP came after X2 and XPAK and it is also smaller.

The newest module standard is the enhanced small form-factor pluggable transceiver, generally called SFP+. Based on the small form-factor pluggable transceiver (SFP) and developed by the ANSI T11 fibre channel group, it is smaller still and lower power than XFP. SFP+ has become the most popular socket on 10GE systems.<sup>[4][5]</sup> SFP+ modules do only optical to electrical conversion, no clock and data recovery, putting a higher burden on the host's channel equalization. SFP+ modules share a common physical form factor with legacy SFP modules, allowing higher port density than XFP and the re-use of existing designs for 24 or 48 ports in a 19" rack width blade.

Optical modules are connected to a host by either a XAUI, XFI or SFI interface. XENPAK, X2, and XPAK modules use XAUI to connect to their hosts. XAUI (XGXS) uses a four-lane data channel and is specified in IEEE 802.3 Clause 48. XFP modules use a XFI interface and SFP+ modules use an SFI interface. XFI and SFI use a single lane data channel and the 64b/66b encoding specified in IEEE 802.3 Clause 49.

SFP+ modules can further be grouped into two types of host interfaces: linear or limiting. Limiting modules are preferred except when using old fiber infrastructure which requires the use of the linear interface provided by 10GBASE-LRM modules.<sup>[6]</sup>

## Optical fiber

There are two classifications for optical fiber: single-mode (SMF) and multi-mode (MMF).<sup>[7]</sup> In SMF light follows a single path through the fiber while in MMF it takes multiple paths resulting in differential mode delay (DMD). SMF is used for long distance communication and MMF is used for distances of less than 300 m. SMF has a narrower core (8.3 μm) which requires a more precise termination and connection method. MMF has a wider core (50 or 62.5 μm). The advantage of MMF is that it can be driven by low cost VCSEL lasers for short distances, and multimode connectors are cheaper and easier to terminate reliably in the field. The advantage of SMF is that it can work over longer distances.<sup>[8]</sup>

In the 802.3 standard reference is made to FDDI-grade MMF fiber. This has a 62.5 μm core and a minimum modal bandwidth of 160 MHz\*km at 850 nm. It was originally installed in the early 1990s for FDDI and 100BaseFX networks. The 802.3 standard also references ISO/IEC 11801 which specifies optical MMF fiber types OM1, OM2, OM3 and OM4. OM1 has a 62.5 μm core while the others have a 50 μm core. At 850 nm the minimum modal bandwidth of OM1 is 200 MHz\*km, of OM2 500 MHz\*km, of OM3 2000 MHz\*km and of OM4 4700 MHz\*km. FDDI-grade cable is now obsolete and new structured cabling installations use either OM3 or OM4 cabling. OM3 cable can carry 10GbE 300 metres using low cost 10GBASE-SR optics (OM4 can manage 400 metres).<sup>[9][10]</sup>

To distinguish SMF from MMF cables, SMF cables are usually yellow, while MMF cables are orange (OM1 & OM2) or aqua (OM3 & OM4). However, in fibre optics there is no agreed colour for any specific optical speed or technology with the exception being angular physical connector (APC), it being an agreed colour of green.<sup>[11]</sup>

There are also active optical cables (AOC). These have the optical electronics already connected eliminating the connectors between the cable and the optical module. They plug into standard optical module sockets. They are lower cost than other optical solutions because the manufacturer can match the electronics to the required length and type of cable.



A Foundry Router with 10 gigabit Ethernet optical interfaces. The yellow cables are single-mode duplex fiber optic connections.

## 10GBASE-SR

10GBASE-SR ("short range") is a port type for multi-mode fiber and uses 850 nm lasers. Its Physical Coding Sublayer 64b/66b PCS is defined in IEEE 802.3 Clause 49 and its Physical Medium Dependent PMD in Clause 52. It delivers serialized data at a line rate of 10.3125 Gbit/s.

Over obsolete FDDI-grade 62.5 micron multi-mode fiber cabling it has a maximum range of 26 metres, over 62.5 micron OM1 it has a range of 33 metres, over 50 micron OM2 a range of 82 metres, over OM3 300 metres and over OM4 400 metres.<sup>[10]</sup> <sup>[12]</sup> OM3 and OM4 are the preferred choices for structured optical cabling within buildings. MMF has the advantage over SMF of having lower cost connectors because of its wider core.

The 10GBASE-SR transmitter is implemented with a vertical-cavity surface-emitting laser (VCSEL) which is low cost and low power. OM3 and OM4 optical cabling is sometimes described as laser optimized because they have been designed to work with VCSELs. 10GBASE-SR delivers the lowest cost, lowest power and smallest form factor optical modules.

For 2011, 10GBASE-SR is projected to make up a quarter of the total 10GbE adapter ports shipped.<sup>[13]</sup>

There is a non-standard lower cost, lower power variant sometimes referred to as 10GBASE-SRL (10GBASE-SR lite). This is inter-operable with 10GBASE-SR but only has a reach of 100 metres.

## 10GBASE-LR

10GBASE-LR ("long reach") is a port type for single-mode fiber and uses 1310 nm lasers. Its Physical Coding Sublayer 64b/66b PCS is defined in IEEE 802.3 Clause 49 and its Physical Medium Dependent PMD in Clause 52. It delivers serialized data at a line rate of 10.3125 Gbit/s.

10GBASE-LR has a specified reach of 10 kilometres (**unknown operator: u'strong'** mi), but 10GBASE-LR optical modules can often manage distances of up to 25 kilometres (**unknown operator: u'strong'** mi) with no data loss.

The 10GBASE-LR transmitter is implemented with a Fabry–Pérot or Distributed feedback laser (DFB). DFB lasers are more expensive than VCSELs but their high power and longer wavelength allow efficient coupling into the small core of single mode fiber over greater distances.

## 10GBASE-LRM

10GBASE-LRM, (Long Reach Multimode) originally specified in IEEE 802.3aq is a port type for multi-mode fiber and uses 1310 nm lasers. Its Physical Coding Sublayer 64b/66b PCS is defined in IEEE 802.3 Clause 49 and its Physical Medium Dependent PMD in Clause 68. It delivers serialized data at a line rate of 10.3125 Gbit/s.

10GBASE-LRM supports distances up to 220 metres (**unknown operator: u'strong'** ft) on FDDI-grade multi-mode fiber and the same 220m maximum reach on OM1, OM2 and OM3 fiber types.<sup>[10]</sup> 10GBASE-LRM reach is not quite as far as the older 10GBASE-LX4 standard.

To ensure that specifications are met over FDDI-grade, OM1 and OM2 fibers, the transmitter should be coupled through a mode conditioning patch cord. No mode conditioning patch cord is required for applications over OM3 or OM4.<sup>[14]</sup>

Some 10GBASE-LRM transceivers also support distances up to 300 metres (**unknown operator: u'strong'** ft) on standard single-mode fiber (SMF, G.652), however this is not part of the IEEE or MSA specification.

10GBASE-LRM uses electronic dispersion compensation (EDC) for receive equalization.<sup>[15]</sup>

10GBASE-LRM has been a failure in the market.<sup>[13]</sup>

## 10GBASE-ER

10GBASE-ER ("extended reach") is a port type for single-mode fiber and uses 1550 nm lasers. Its Physical Coding Sublayer 64b/66b PCS is defined in IEEE 802.3 Clause 49 and its Physical Medium Dependent PMD in Clause 52. It delivers serialized data at a line rate of 10.3125 Gbit/s.

The 10GBASE-ER transmitter is implemented with an externally modulated laser (EML).

10GBASE-ER has a reach of 40 kilometres (**unknown operator: u'strong'** mi) over engineered links and 30 km over standard links.<sup>[10][16]</sup>

## 10GBASE-ZR

Several manufacturers have introduced 80 km (**unknown operator: u'strong'** mi) range ER pluggable interfaces under the name 10GBASE-ZR. This 80 km PHY is not specified within the IEEE 802.3ae standard and manufacturers have created their own specifications based upon the 80 km PHY described in the OC-192/STM-64 SDH/SONET specifications.

The 802.3 standard will not be amended to cover the ZR PHY.

## 10GBASE-LX4

10GBASE-LX4 is a port type for multi-mode fiber and single-mode fiber. It uses four separate laser sources operating at 3.125 Gbit/s and coarse WDM with four unique wavelengths around 1310 nm. Its Physical Coding Sublayer 8B10B PCS is defined in IEEE 802.3 Clause 48 and its Physical Medium Dependent PMD in Clause 53.<sup>[10]</sup>

It supports a range of 300 metres (**unknown operator: u'strong'** ft) over FDDI-grade, OM1, OM2 and OM3 multi-mode cabling (all these fiber types are specified to have a minimum modal bandwidth of 500 MHz\*km at 1300 nm).

10GBASE-LX4 also supports a range of 10 kilometres (**unknown operator: u'strong'** mi) over SMF.

For MMF links the WDM output needs to be coupled through a SMF offset-launch mode-conditioning patch cord. This is explained in subclauses 53.6 and 38.11.4 of the IEEE 802.3 spec.<sup>[10]</sup>

Until 2005 10GBASE-LX4 optical modules were cheaper than 10GBASE-LR optical modules.

10GBASE-LX4 was used by people who wanted to support both MMF and SMF with a single optical module.

10GBASE-LX4 is now an obsolete technology and has no significant market presence.

## Copper

10G Ethernet can also run over twin-ax cabling, twisted pair cabling, and backplanes.

## 10GBASE-CX4

**10GBASE-CX4** — was the first 10G copper standard published by 802.3 (as 802.3ak-2004). It uses the XAUI 4-lane PCS (Clause 48) and copper cabling similar to that used by InfiniBand technology. It is specified to work up to a distance of 15 m (**unknown operator: u'strong'** ft). Each lane carries 3.125 G baud of signaling bandwidth.

10GBASE-CX4 offers the advantages of low power, low cost and low latency, but has a bigger form factor and more bulky cables than the newer single lane SFP+ standard and a much shorter reach than fibre or 10GBASE-T.

Shipments of 10GBASE-CX4 today are very low.<sup>[13]</sup>

## SFP+ Direct Attach

Also known as 10GSFP+Cu, 10GBase-CR, or 10GBase-CX1, SFP+, or 10GbE Cu SFP cables. Direct Attach uses a passive twin-ax cable assembly and connects directly into an SFP+ housing. SFP+ Direct Attach has a fixed-length cable, typically 3, 5 or 7m in length, and like 10GBASE-CX4, is low power, low cost and low latency with the added advantages of using less bulky cables and of having the small form factor of SFP+. SFP+ Direct Attach today is tremendously popular, with more ports installed than 10GBASE-SR.<sup>[13]</sup>

## Backplane

**Backplane Ethernet** — also known by its task force name **802.3ap** — is used in backplane applications such as blade servers and routers/switches with upgradable line cards. 802.3ap implementations are required to operate in an environment comprising up to 1 metre (**unknown operator: u'strong'** in) of copper printed circuit board with two connectors. The standard defines two port types for 10 Gbit/s (**10GBASE-KX4** and **10GBASE-KR**) and a 1 Gbit/s port type (1000BASE-KX). It also defines an optional layer for FEC, a backplane autonegotiation protocol and link training for 10GBASE-KR where the receiver can set a three tap transmit equalizer. The autonegotiation protocol selects between 1000BASE-KX, 10GBASE-KX4, 10GBASE-KR or 40GBASE-KR4 operation. 40GBASE-KR4 is defined in 802.3ba.<sup>[17]</sup>

New backplane designs use 10GBASE-KR rather than 10GBASE-KX4.<sup>[13]</sup>

### 10GBASE-KX4

This operates over four backplane lanes and uses the same physical layer coding (defined in IEEE 802.3 Clause 48) as 10GBASE-CX4.

### 10GBASE-KR

This operates over a single backplane lane and uses the same physical layer coding (defined in IEEE 802.3 Clause 49) as 10GBASE-LR/ER/SR.

### 10GBASE-T

**10GBASE-T**, or **IEEE 802.3an-2006**, is a standard released in 2006 to provide 10 Gbit/s connections over unshielded or shielded twisted pair cables, over distances up to 100 metres (**unknown operator: u'strong'** ft).<sup>[18]</sup> 10GBASE-T cable infrastructure can also be used for 1000BASE-T allowing a gradual upgrade from 1000BASE-T using autonegotiation to select which speed to use. 10GBASE-T has latency in the range 2 to 4 microseconds compared to 1 to 12 microseconds on 1000BASE-T.<sup>[19][20]</sup> As of 2010 10GBASE-T silicon is available from several manufacturers<sup>[21][22][23][24]</sup> with claimed power dissipation of 3-4 W at structure widths of 40 nm. and with 28 nm in development, power will continue to decline.

10GBASE-T uses the IEC 60603-7 8P8C (commonly known as RJ45) connectors already widely used with Ethernet. Transmission characteristics are now specified to 500 MHz. To reach this frequency Category 6A or better balanced twisted pair cables specified in ISO/IEC 11801 amendment 2 or ANSI/TIA-568-C.2 are needed to carry 10GBASE-T up to distances of 100 m. Category 6 cables can carry 10GBASE-T for shorter distances when qualified according to the guidelines in ISO TR 24750 or TIA-155-A.

### Electrical characteristics

The 802.3an standard defines the wire-level modulation for 10GBASE-T as a Tomlinson-Harashima precoded (THP) version of pulse-amplitude modulation with 16 discrete levels (PAM-16), encoded in a two-dimensional checkerboard pattern known as DSQ128. Several proposals were considered for wire-level modulation, including PAM with 12 discrete levels (PAM-12), 10 levels (PAM-10), or 8 levels (PAM-8), both with and without Tomlinson-Harashima Precoding (THP). PAM-5 is what is used in the older 1000BASE-T gigabit Ethernet standard.

## WAN PHY (10GBASE-W)

The WAN PHY uses the 10GBASE-S, 10GBASE-L and 10GBASE-E optical PMDs and is designated as 10GBASE-SW, 10GBASE-LW or 10GBASE-EW. Its Physical Coding Sublayer 64b/66b PCS is defined in IEEE 802.3 Clause 49 and its Physical Medium Dependent PMDs in Clauses 52. It also uses a WAN Interface Sublayer (WIS) defined in Clause 50 which adds extra encapsulation to format the frame data to be compatible with SONET STS-192c.<sup>[10]</sup>

The WAN PHY was designed to interoperate with OC-192/STM-64 SDH/SONET equipment using a light-weight SDH/SONET frame running at 9.953 Gbit/s.

## 10GbE NICs

10GbE network interface cards are available from several manufacturers. These plug into ordinary computer servers using PCI express and connect to the LAN with a choice of PHY modules.

## Notes and references

- [1] Anil Sharma (January 19, 2011). "LightCounting forecasts CAGR of Over 300 Percent for 10GBASE-T Port Shipments Through 2014" (<http://10-gigabit-ethernet.tmcnet.com/topics/10-gigabit-ethernet/articles/136124-lightcounting-forecasts-cagr-over-300-percent-10gbase-t.htm>). TMCnet. . Retrieved May 7, 2011.
- [2] "Dell'Oro press release" (<http://www.delloro.com/news/2010/ES022210.htm>). . Retrieved 29 March 2011.
- [3] "Intel blog about Interop 2011" (<http://communities.intel.com/community/openportit/server/blog/2011/05/12/overheard-at-interop-a-few-questions-about-ethernet>). . Retrieved 20 September 2011.
- [4] "LightCounting's LightTrends April 2010" (<http://www.lightcounting.com/lighttrends/1004/>). . Retrieved 03 May 2010.
- [5] "10GbE Optical Component and SFP+ Modules: This Time It's Different by Andrew Schmitt" (<http://www.nyquistcapital.com/2007/11/28/10gbe-and-sfp-this-time-its-different>). . Retrieved 11 March 2008.
- [6] "The road to SFP+: Examining module and system architectures by Ryan Latchman and Bharat Tailor" ([http://lw.pennnet.com/display\\_article/317903/13/ARTCL/none/OTRAT/1/The-road-to-SFP+-Examining-module-and-system-architectures](http://lw.pennnet.com/display_article/317903/13/ARTCL/none/OTRAT/1/The-road-to-SFP+-Examining-module-and-system-architectures)). . Retrieved 15 January 2009.
- [7] "Optical Fiber and 10 gigabit Ethernet white paper by the 10GEA" (<http://web.archive.org/web/20080614015352/http://www.10gea.org/optical-fiber-10ge.htm>). Archived from the original (<http://www.10gea.org/optical-fiber-10ge.htm>) on 14 June 2008. . Retrieved 01 July 2008.
- [8] "Why choose Multimode fiber? by Corning" (<http://www.corning.com/docs/opticalfiber/cn0603.pdf>). . Retrieved 11 March 2008.
- [9] "10 Gigabit Ethernet over Multimode Fiber by John George" (<http://bicsi.org/Events/Conferences/Spring/2005/GeorgePRES.pdf>). . Retrieved 10 March 2008.
- [10] "IEEE 802.3 standard" (<http://web.archive.org/web/20070826151712/http://standards.ieee.org/getieee802/802.3.html>). Archived from the original (<http://standards.ieee.org/getieee802/802.3.html>) on 26 August 2007. . Retrieved 14 August 2007.
- [11] "How to tell? MMF or SMF" (<http://www.velocityreviews.com/forums/t33419-how-to-tell-mmf-or-smf.html>). . Retrieved 06 September 2011.
- [12] "Description of Cisco 10G optical modules" ([http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6574/product\\_data\\_sheet0900aecdb01f92aa.html](http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6574/product_data_sheet0900aecdb01f92aa.html)). . Retrieved 03 May 2010.
- [13] "Another Serving of Alphabet Soup — by Intel" (<http://communities.intel.com/community/openportit/server/blog/2011/06/20/10-gigabit-ethernet-update-another-serving-of-alphabet-soup>). . Retrieved 04 September 2011.
- [14] "Cisco 10GBASE SFP+ Modules Data Sheet" ([http://www.cisco.com/en/US/prod/collateral/modules/ps5455/data\\_sheet\\_c78-455693.html](http://www.cisco.com/en/US/prod/collateral/modules/ps5455/data_sheet_c78-455693.html)). Cisco Systems. February 2012. . Retrieved 2012-05-12.
- [15] "10GBase-LX4 vs 10GBase-LRM: A debate" ([http://lw.pennnet.com/display\\_article/249488/13/ARTCL/none/none/1/10GBase-LX4-vs-10GBase-LRM:-A-debate](http://lw.pennnet.com/display_article/249488/13/ARTCL/none/none/1/10GBase-LX4-vs-10GBase-LRM:-A-debate)). Archived (<http://www.webcitation.org/5iQGmo2yv>) from the original on 2009-07-20. . Retrieved 2009-07-16.
- [16] "Cisco 10GBASE XENPAK Modules" ([http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product\\_data\\_sheet09186a008007cd00\\_ps5251\\_Products\\_Data\\_Sheet.html](http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a008007cd00_ps5251_Products_Data_Sheet.html)). Cisco Systems. November 2011. . Retrieved 2012-05-12.
- [17] "IEEE P802.3ap Backplane Ethernet Task Force" (<http://grouper.ieee.org/groups/802/3/ap/index.html>). . Retrieved 30 January 2011.
- [18] "IEEE Standards Status Report for 802.3an" (<http://standards.ieee.org/cgi-bin/status?802.3an>). . Retrieved 14 August 2007.
- [19] "10GBASE-T for Broad 10 Gigabit Adoption in the Data Center" ([http://download.intel.com/support/network/sb/intel\\_ether\\_10gbaset.pdf](http://download.intel.com/support/network/sb/intel_ether_10gbaset.pdf)), Intel, , retrieved 2011-12-21
- [20] "SWITCHES SWITCH FROM 1000BASE-T TO 10GBASE-T NOW" ([http://www.plxtech.com/files/pdf/support/10gbaset/whitepapers/10GBase-T\\_1000Base-T\\_Switches.pdf](http://www.plxtech.com/files/pdf/support/10gbaset/whitepapers/10GBase-T_1000Base-T_Switches.pdf)), Teranetics, October 2009, , retrieved 2011-12-21

- [21] "Broadcom 10GBASE-T PHY" (<http://www.broadcom.com/products/Physical-Layer/10-Gigabit-Ethernet-PHYs>). . Retrieved 02 December 2011.
- [22] "PLX Technology, Teranetics 10GBASE-T PHY" (<http://www.plxtech.com/products/10gbase-t>). . Retrieved 11 February 2011.
- [23] "Solar Flare 10GBASE-T PHY" (<http://www.solarflare.com/products/10xpress.php>). Archived (<http://www.webcitation.org/5jc2TUnO0>) from the original on 2009-09-07. . Retrieved 2009-09-05.
- [24] "Aquantia 10GBASE-T PHY" ([http://web.archive.org/web/20081203093838/http://www.aquantia.com/pdf/AquantiaAQ1002\\_11172008.pdf](http://web.archive.org/web/20081203093838/http://www.aquantia.com/pdf/AquantiaAQ1002_11172008.pdf)). Archived from the original ([http://www.aquantia.com/pdf/AquantiaAQ1002\\_11172008.pdf](http://www.aquantia.com/pdf/AquantiaAQ1002_11172008.pdf)) on 03 December 2008. . Retrieved 10 December 2008.

## External links

- Full text of the IEEE 802.3 standard (<http://standards.ieee.org/getieee802/802.3.html>)
- IEEE 802.3 Ethernet Working Group (<http://www.ieee802.org/3/>)
- Ethernet Alliance website (<http://www.ethernetalliance.org>)
- University of New Hampshire Interoperability Laboratory 10 Gigabit Ethernet Consortium (<http://www.iol.unh.edu/consortiums/10gec/>)
- First global independent comparative 3rd party UTP-STP study (<http://www.utp-vs-stp.com/web/Microsites/UTP-vs-STP/>)
- Description of SFP+ Direct Attach server NIC in top-of-rack concept ([http://www.intel.com/Assets/PDF/prodbrief/Intel\\_10\\_Gig\\_AFDA\\_Dual\\_Port\\_prodbrief.pdf](http://www.intel.com/Assets/PDF/prodbrief/Intel_10_Gig_AFDA_Dual_Port_prodbrief.pdf))

# 100 Gigabit Ethernet

**100 Gigabit Ethernet** (or **100GbE**) and **40 Gigabit Ethernet** (or **40GbE**) are high-speed computer network standards developed by the Institute of Electrical and Electronics Engineers (IEEE).<sup>[1]</sup> They support sending Ethernet frames at 40 and 100 gigabits per second over multiple 10 Gbit/s or 25 Gbit/s lanes. Previously, the fastest published Ethernet standard was 10 Gigabit Ethernet. They were first studied in November 2007, proposed as IEEE 802.3ba in 2008, and ratified in June 2010.<sup>[2]</sup> Another variant was added in March 2011.

## History

In June 2007, a trade group called "Road to 100G" was formed after the NXTcomm trade show in Chicago.<sup>[3]</sup> Official standards work was started by IEEE 802.3 Higher Speed Study Group.<sup>[4]</sup> The P802.3ba Ethernet Task Force commenced on December 5, 2007<sup>[5]</sup> with the following project authorization request:

The purpose of this project is to extend the 802.3 protocol to operating speeds of 40 Gb/s and 100 Gb/s in order to provide a significant increase in bandwidth while maintaining maximum compatibility with the installed base of 802.3 interfaces, previous investment in research and development, and principles of network operation and management. The project is to provide for the interconnection of equipment satisfying the distance requirements of the intended applications.

## Physical standards

The 40/100 Gigabit Ethernet standards encompass a number of different Ethernet physical layer (PHY) specifications. A networking device may support different PHY types by means of pluggable modules. Optical modules are not standardized by any official standards body but are in multi-source agreements (MSAs). One agreement that supports 40 and 100 Gigabit Ethernet is the C Form-factor Pluggable (CFP) MSA<sup>[6]</sup> which was adopted for distances of 100+ meters. QSFP and CXP connector modules support shorter distances.<sup>[7]</sup>

The standard supports only full-duplex operation.<sup>[8]</sup> Other electrical objectives include:

- Preserve the 802.3 / Ethernet frame format utilizing the 802.3 MAC

- Preserve minimum and maximum FrameSize of current 802.3 standard
- Support a bit error ratio (BER) better than or equal to  $10^{-12}$  at the MAC/PLS service interface
- Provide appropriate support for OTN
- Support MAC data rates of 40 and 100 Gbit/s
- Provide Physical Layer specifications (PHY) for operation over single-mode optical fiber (SMF), laser optimized multi-mode optical fiber (MMF) OM3 and OM4, copper cable assembly, and backplane.

The following nomenclature was used for the physical layers:<sup>[9]</sup>

Physical layer	40 Gigabit Ethernet	100 Gigabit Ethernet
Backplane	40GBASE-KR4	
Copper cable	40GBASE-CR4	100GBASE-CR10
100 m over OM3 MMF	40GBASE-SR4	100GBASE-SR10
125 m over OM4 MMF <sup>[7]</sup>		
10 km over SMF	40GBASE-LR4	100GBASE-LR4
40 km over SMF		100GBASE-ER4
Serial SMF over 2 km	40GBASE-FR	

The 100 m laser optimized multi-mode fiber (OM3) objective was met by parallel ribbon cable with 850 nm wavelength 10GBASE-SR like optics (40GBASE-SR4 and 100GBASE-SR10). The backplane objective with 4 lanes of 10GBASE-KR type PHYs (40GBASE-KR4). The copper cable objective is met with 4 or 10 differential lanes using SFF-8642 and SFF-8436 connectors. The 10 and 40 km 100G objectives with four wavelengths (around 1310 nm) of 25G optics (100GBASE-LR4 and 100GBASE-ER4) and the 10 km 40G objective with four wavelengths (around 1310 nm) of 10G optics (40GBASE-LR4).<sup>[10]</sup>

In January 2010 another IEEE project authorization started a task force to define a 40 gigabit per second serial single-mode optical fiber standard (40GBASE-FR). This was approved as standard 802.3bg in March 2011.<sup>[11]</sup> It used 1550 nm optics, had a reach of 2 km and was capable of receiving 1550 nm and 1310 nm wavelengths of light. The capability to receive 1310 nm light allows it to inter-operate with a longer reach 1310 nm PHY should one ever be developed. 1550 nm was chosen as the wavelength for 802.3bg transmission to make it compatible with existing test equipment and infrastructure.<sup>[12]</sup>

In December 2010, a 10x10 Multi Source Agreement (10x10 MSA) began to define an optical Physical Medium Dependent (PMD) sublayer and establish compatible sources of low-cost, low-power, pluggable optical transceivers based on 10 optical lanes at 10 gigabits/second each.<sup>[13]</sup> The 10x10 MSA was intended as a lower cost alternative to 100GBASE-LR4 for applications which do not require a link length longer than 2 km. It was intended for use with standard single mode G.652.C/D type low water peak cable with ten wavelengths ranging from 1523 to 1595 nm. The founding members were Google, Brocade Communications, JDSU and Santur.<sup>[14]</sup> Other member companies of the 10x10 MSA included MRV, Enablence, Cyoptics, AFOP, OPLINK, Hitachi Cable America, AMS-IX, EXFO, Huawei, Kotura, Facebook and Effdon when the 2 km specification was announced in March 2011.<sup>[15]</sup> The 10X10 MSA modules were intended to be the same size as the C Form-factor Pluggable specifications.

## Backplane

NetLogic Microsystems announced backplane modules in October 2010.<sup>[16]</sup> This industry trend is important because standards-based 100GE interconnects may allow building optical backplanes at a fraction of price currently required by VCSEL based implementations – such as those found in multichassis systems from Cisco (CRS) and Juniper Networks (T-series).

## Copper cables

Quellan announced a test board,<sup>[17]</sup> but no module is available.

## Multimode fiber

In 2009, Mellanox<sup>[18]</sup> and Reflex Photonics<sup>[19]</sup> announced modules based on the CFP agreement.

## Single mode fiber

Finisar,<sup>[20]</sup> Sumitomo Electric Industries,<sup>[21]</sup> and OpNext<sup>[22]</sup> all demonstrated singlemode 40 or 100 Gigabit Ethernet modules based on the C Form-factor Pluggable agreement at the European Conference and Exhibition on Optical Communication in 2009.

## Compatibility

Optical domain IEEE 802.3ba implementations were not compatible with the numerous 40G and 100G line rate transport systems which feature different optical layer and modulation formats. In particular, existing 40 Gigabit transport solutions that used dense wavelength-division multiplexing to pack four 10 Gigabit signals into one optical medium were not compatible with the IEEE 802.3ba standard, which used either coarse WDM in 1310 nm wavelength region with four 25 Gigabit or four 10 Gigabit channels, or parallel optics with four or ten optical fibers per direction.

## Test and Measurement

Ixia developed Physical Coding Sublayer Lanes<sup>[23]</sup> and demonstrated a working 100GbE link through a test setup at NXTcomm in June 2008.<sup>[24]</sup> Ixia announced test equipment in November 2008.<sup>[25][26]</sup>

Discovery Semiconductors introduced optoelectronics converters for 100 gigabit testing of the 10 km and 40 km Ethernet standards in February 2009.<sup>[27]</sup>

JDS Uniphase introduced test and measurement products for 40 and 100 Gigabit Ethernet in August 2009.<sup>[28]</sup>

Spirent Communications introduced test and measurement products in September 2009.<sup>[29]</sup>

EXFO demonstrated interoperability in January 2010.<sup>[30]</sup>

Xena Networks demonstrated test equipment at the Technical University of Denmark in January 2011.<sup>[31][32]</sup>

These products verify Ethernet protocol implementation but do not test physical layer compliance to IEEE PMD specifications.

## First commercial 100GE trials and deployments

Although 100GE is a commodity interface in 2012 and beyond, it helps to understand the timeline and drivers behind the commercial adoption of technology.

Unlike the "race to 10Gbps" that was driven by the imminent needs to address growth pains of Internet in late 1990s, customer interest in 100Gbit/s technologies was mostly driven by economic factors. Among those, the common reasons to adopt 100GE were:<sup>[33]</sup>

- to reduce the number of optical wavelengths ("lambdas") used and the need to light new fiber
- to utilize bandwidth more efficiently than 10Gbit/s link aggregates
- to provide cheaper wholesale, internet peering and data center interconnect connectivity
- to skip the relatively expensive 40Gbit/s technology and move directly from 10Gbit/s to 100Gbit/s

Considering that 100GE technology is natively compatible with OTN hierarchy and there is no separate adaptation for SONET/SDH and Ethernet networks, it was widely believed that 100GE technology adoption will be driven by products in all network layers, from transport systems to edge routers and datacenter switches. Nevertheless, in 2011 components for 100GE networks were not a commodity and most vendors entering this market relied on both internal R&D projects and extensive cooperation with other companies.

## Optical Transport Systems

Solving the challenges of optical signal transmission over a nonlinear medium is principally an analog design problem. As such, it has evolved at a slower rate relative to digital circuit lithography advances (which have generally progressed in step with Moore's law.) This explains why 10Gbit/s transport systems have existed since the mid-1990s, while the first forays into 100Gbit/s transmission happened about 15 years later – a 10x speed increase over 15 years is far slower than the 2x speed per 1.5 years typically cited for Moore's law tracking technologies. Nevertheless, as of Aug 2011 at least five firms (Ciena, Alcatel-Lucent, MRV, ADVA Optical and Huawei) have made customer announcements for 100Gbit/s transport systems<sup>[34]</sup> – although with varying degrees of capabilities. Although most vendors claim that 100Gbit/s lightpaths can utilize existing analog optical infrastructure, in practice deployment of new, high-speed lambdas remains tightly controlled and extensive interoperability tests are required before moving new capacity into service.

## Routers and switches with 100GbE interfaces

Design of router or switch with support for 100Gbit/s interfaces is not an easy feat for multiple reasons. One of them is the need to process a 100Gbit/s stream of packets at line rate without reordering within IP/MPLS microflows. As of 2011, most components in the 100Gbit/s packet processing path (PHY chips, NPUs, memories) were not readily available off-the-shelf or require extensive qualification and co-design. Another problem is related to the low-output production of 100Gbit/s optical components, which were also not easily available – especially in pluggable, long-reach or tunable laser flavors.

### Alcatel-Lucent

Alcatel-Lucent first announced 100GbE interfaces for their 7450 ESS/7750 SR platform in June 2009, with field trials following in June–September 2010.<sup>[35]</sup> However, in April 2011 presentation, James Watt (ALU optical division president) still mentioned 100GbE technology as "demo" staged for T-Systems and Portugal Telecom.<sup>[36]</sup> Later, in a June 2011 press-release with Verizon, the company again referenced 100GbE as "trial"<sup>[37]</sup> Thus, despite of being able to bundle the self-developed optical and routing system, Alcatel apparently missed the chance to book early revenue with 100GbE deployments.

In a separate press release from June 2011, Alcatel-Lucent announced a packet processing architecture dubbed FP3.<sup>[38]</sup>

P&T Luxembourg took in service 100G circuits between Luxemburg and Frankfurt in September 2011 on 1830 from Alcatel-Lucent.<sup>[39]</sup> <sup>[40]</sup> <sup>[41]</sup>

### **Brocade Communications Systems**

In September 2010, Brocade announced their first 100GbE products to be based on the former Foundry Networks hardware (MLXe).<sup>[42]</sup> In June 2011, the new product went live at AMS-IX traffic exchange point in Amsterdam,<sup>[43]</sup> bringing first-ever 100GbE revenue for Brocade.

### **Cisco Systems**

The joint Cisco-Comcast press release on their first 100GbE trials was released in June 2008,<sup>[44]</sup> however it is doubtful this transmission could approach 100Gbit/s speeds when using a 40Gbit/s/per slot CRS-1 platform for packet processing. Cisco's first deployment of 100GbE at AT&T and Comcast occurred in April 2011.<sup>[45]</sup> Later in the same year, Cisco tested the 100GbE interface between CRS-3 and a new generation of their ASR9K edge router.<sup>[46]</sup>

### **Huawei**

In October 2008, the Chinese vendor presented their first 100GbE interface for their flagship router, NE5000e.<sup>[47]</sup> In September 2009, Huawei also presented an end-to-end 100G solution consisting of OSN6800/8800 optical transport and 100GbE ports on NE5000e.<sup>[48]</sup> This time, it was also mentioned that Huawei's products had the new self-developed NPU "Solar 2.0 PFE2A" onboard and was using pluggable optics in CFP form-factor. In a mid-2010 product brief, the new NE5000e linecards were given commercial name (LPUF-100) and were credited with using two Solar-2.0 NPUs per 100GbE port in opposite (ingress/egress) configuration.<sup>[49]</sup> Nevertheless, in October 2010, the company referenced shipments of NE5000e to Russian cell operator "Megafon" as "40Gbps/slot" solution, with "scalability up to" 100Gbit/s.<sup>[50]</sup>

In April 2011, Huawei announced that the NE5000e platform was updated to carry 2x100GbE interfaces per slot using LPU-200 linecards.<sup>[51]</sup> In a related solution brief, Huawei reported 120 thousand 20G/40G Solar 1.0 chips as shipped to customers, but no Solar 2.0 numbers were given.<sup>[52]</sup> Also, following the August 2011 100G trial in Russia, Huawei reported paying 100G DWDM customers, but no 100GbE shipments on NE5000e.<sup>[53]</sup>

### **Juniper Networks**

Juniper first announced that 100GbE would come to its T-series routers in June 2009.<sup>[54]</sup> The 1x100GbE option followed in Nov 2010, when a joint press release with academic backbone network Internet2 marked the first production 100GbE interfaces going live in real network.<sup>[55]</sup> Later in the same year, Juniper demonstrated 100GbE operation between core (T-series) and edge (MX 3D) routers.<sup>[56]</sup> Juniper, in March 2011, announced first shipments of 100GbE interfaces to a major North American service provider (Verizon<sup>[57]</sup>). In April 2011, Juniper successfully deployed a 100GbE system to an operator in the UK.(JANET<sup>[58]</sup>).

## Standardization time line

IEEE standardization project history:

- Call for interest at IEEE 802.3 plenary meeting in San Diego – July 18, 2006
- First HSSG study group meeting – September 2006
- Last study group meeting – November 2007
- Task Force formally approved as P802.3ba by IEEE LMSC – December 5, 2007
- First P802.3ba task force meeting – January 2008
- IEEE 802.3 working group ballot – March 2009
- IEEE LMSC sponsor ballot – November 2009
- First 40 Gbit/s Ethernet Single-mode Fibre PMD study group meeting – January 2010.<sup>[59]</sup>
- P802.3bg task force approved for 40 Gbit/s serial SMF PMD— March 25, 2010
- IEEE 802.3ba standard approved – June 17, 2010<sup>[1][60]</sup>
- IEEE 802.3bg standard approved – March 2011<sup>[11]</sup>
- IEEE 802.3bj 100 Gbit/s Backplane and Copper Cable Task Force PAR approval due – September 2011

P802.3ba Task Force draft release dates:

- Draft 1.0 – October 1, 2008
- Draft 1.1 – December 9, 2008
- Draft 1.2 – February 10, 2009
- Draft 2.0 – March 12, 2009 (for working group ballot)
- Draft 2.1 – May 29, 2009
- Draft 2.2 – August 15, 2009
- Draft 2.3 – October 14, 2009
- Draft 3.0 – November 18, 2009 (for sponsor group ballot)<sup>[61]</sup>
- Draft 3.1 – February 10, 2010
- Draft 3.2 – March 24, 2010
- Final – June 17, 2010<sup>[60]</sup>

## References

- [1] "IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force" (<http://www.ieee802.org/3/ba/>). *official web site*. IEEE. June 19, 2010. . Retrieved June 24, 2011.
- [2] Reimer, Jeremy (July 25, 2007). "New Ethernet standard: not 40Gbps, not 100, but both" (<http://arstechnica.com/hardware/news/2007/07/new-etherent-standard-not-40-gbps-not-100-but-both.ars>). Ars Technica. . Retrieved December 17, 2011.
- [3] Jeff Caruso (June 21, 2007). "Group pushes 100 Gigabit Ethernet: The 'Road to 100G' Alliance is born" (<http://www.networkworld.com/newsletters/lans/2007/0618lan2.html>). *Network World*. . Retrieved June 6, 2011.
- [4] "IEEE 802.3 Higher Speed Study Group" (<http://www.ieee802.org/3/hssg/>). IEEE802.org. . Retrieved December 17, 2011.
- [5] "Project Authorization Request Approval notification: Approval of P802.3ba" ([http://www.ieee802.org/3/ba/PAR/par\\_0308.pdf](http://www.ieee802.org/3/ba/PAR/par_0308.pdf)). IEEE Standards Association Standards Board. December 5, 2007. . Retrieved June 6, 2011.
- [6] "CFP Multi-Source Agreement" (<http://www.cfp-msa.org/>). *official web site*. Archived (<http://www.webcitation.org/5k781ouJn>) from the original on September 27, 2009. . Retrieved June 24, 2011.
- [7] Greg Hankins (October 20, 2009). "IEEE P802.3ba 40 GbE and 100 GbE Standards Update" ([http://www.nanog.org/meetings/nanog47/presentations/Tuesday/Hankins\\_IEEE\\_N47\\_Tues.pdf](http://www.nanog.org/meetings/nanog47/presentations/Tuesday/Hankins_IEEE_N47_Tues.pdf)) (PDF). *North American Network Operators' Group (NANOG) 47 Presentations*. . Retrieved June 24, 2011.
- [8] John D'Ambrosia. "IEEE P802.3ba Objectives" ([http://www.ieee802.org/3/ba/PAR/P802.3ba\\_Objectives\\_0709.pdf](http://www.ieee802.org/3/ba/PAR/P802.3ba_Objectives_0709.pdf)). Archived (<http://www.webcitation.org/5k77zCcGc>) from the original on September 27, 2009. . Retrieved September 25, 2009.
- [9] Ilango Ganga (May 13, 2009). "Chief Editor's Report" ([http://www.ieee802.org/3/ba/public/may08/ganga\\_02\\_0508.pdf](http://www.ieee802.org/3/ba/public/may08/ganga_02_0508.pdf)). *IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force public record. p. 8.* . Retrieved June 7, 2011.
- [10] Ilango Ganga; Brad Booth; Howard Frazier; Shimon Muller; Gary Nicholl (May 13, 2008). "IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force, May 2008 Meeting" (<http://www.ieee802.org/3/ba/public/may08/index.htm>). .
- [11] "IEEE P802.3bg 40Gb/s Ethernet: Single-mode Fibre PMD Task Force" (<http://www.ieee802.org/3/bg/>). *official task force web site*. IEEE 802. April 12, 2011. . Retrieved June 7, 2011.

- [12] Anderson, Jon. "Rationale for dual-band Rx in 40GBASE-FR" ([http://www.ieee802.org/3/bg/public/nov10/anderson\\_01a\\_1110.pdf](http://www.ieee802.org/3/bg/public/nov10/anderson_01a_1110.pdf)). .
- [13] "10 x 10 MSA – Low Cost 100 GB/s Pluggable Optical Transceiver" (<http://www.10x10msa.org>). *official web site.* 10x10 multi-source agreement. . Retrieved June 24, 2011.
- [14] "Leading Industry Peers Join Forces to Develop Low-Cost 100G Multi-Source Agreement" (<http://www.businesswire.com/news/home/20101207005672/en>). *Businesswire news release.* December 7, 2010. . Retrieved June 24, 2011.
- [15] "10X10 MSA Ratifies Specification for Low Cost 100 Gb/s 2 Kilometer Links" ([http://www.10x10msa.org/press\\_releases/10x10MSA\\_public\\_specification\\_released.pdf](http://www.10x10msa.org/press_releases/10x10MSA_public_specification_released.pdf)). *News release* (10x10 MSA). March 4, 2011. . Retrieved June 24, 2011.
- [16] "NetLogic Microsystems Announces Industry's First Dual-Mode Quad-Port 10GBASE-KR and 40GBASE-KR4 Backplane PHY with Energy Efficient Ethernet" (<http://investors.netlogicmicro.com/phoenix.zhtml?c=178551&p=irol-newsArticle&ID=1482016>). *News release* (NetLogic Microsystems). October 13, 2010. . Retrieved June 7, 2011.
- [17] "Quellan QLx411GRx 40G Evaluation Board" ([http://www.quellan.com/products/qlx411grx\\_eval\\_board.html](http://www.quellan.com/products/qlx411grx_eval_board.html)). Archived (<http://www.webcitation.org/5k780AjC4>) from the original on September 27, 2009. . Retrieved September 25, 2009.
- [18] "Mellanox Technologies" ([http://www.mellanox.com/content/pages.php?pg=press\\_release\\_item&rec\\_id=350](http://www.mellanox.com/content/pages.php?pg=press_release_item&rec_id=350)). Archived (<http://www.webcitation.org/5k780apsR>) from the original on September 27, 2009. . Retrieved September 25, 2009.
- [19] "InterBOARD CFP 100GBASE-SR10 Parallel Optical Module" (<http://www.webcitation.org/5k7810hE5>). *commercial web site.* Reflex Photonics Inc.. Archived from the original (<http://www.reflexphotonics.com/interboard-cfp.htm>) on September 27, 2009. . Retrieved June 7, 2011.
- [20] "Finisar Corporation – Finisar First to Demonstrate 40 Gigabit Ethernet LR4 CFP Transceiver Over 10 km of Optical Fiber at ECOC" (<http://investor.finisar.com/releasedetail.cfm?ReleaseID=410286>). Archived (<http://www.webcitation.org/5k781NpJi>) from the original on September 27, 2009. . Retrieved September 25, 2009.
- [21] "Sumitomo Electric develops 40GbE transceiver" (<http://www.lightwaveonline.com/top-stories/Sumitomo-Electric-develops-40GbE-transceiver--60446587.html>). . Retrieved September 25, 2009.
- [22] "Hitachi and Opnext unveil receiver for 100GbE and demo 10 km transmission over SMF" ([http://www.semiconductor-today.com/news\\_items/2009/APRIL/OPNEXT\\_030409.htm](http://www.semiconductor-today.com/news_items/2009/APRIL/OPNEXT_030409.htm)). . Retrieved October 26, 2009.
- [23] "Enabling 100 Gigabit Ethernet Implementing PCS Lanes" ([http://www.ixiacom.com/pdfs/library/white\\_papers/PCS\\_white\\_paper.pdf](http://www.ixiacom.com/pdfs/library/white_papers/PCS_white_paper.pdf)). .
- [24] "Avago Technologies, Infinera & Ixia to demo the first 100 Gig Ethernet" (<http://www.youtube.com/watch?v=WD20eVtGTCs>). Archived (<http://www.webcitation.org/662ziTse6>) from the original on 2012-03-09. . Retrieved 7 March 2012.
- [25] "Ixia First to Offer 100 GE Testing Capability" ([http://www.ixiacom.com/news\\_and\\_events/press\\_releases/display.php?skey=209](http://www.ixiacom.com/news_and_events/press_releases/display.php?skey=209)). *News release* (Ixia). September 29, 2008. . Retrieved June 7, 2011.
- [26] "40 Gb/s and 100 Gb/s Testing: Overview" ([http://www.ixiacom.com/products/higher\\_speed\\_ethernet\\_testing/index.php](http://www.ixiacom.com/products/higher_speed_ethernet_testing/index.php)). *commercial web site.* Ixia. . Retrieved June 7, 2011.
- [27] "Discovery Semiconductors – 100 Gb Ethernet (4 x 25 Gb/s) Quad PIN-TIA Optical Receiver" (<http://discoverysemi.com/Product Pages/DSCR801.php>). *commercial web site.* . Retrieved June 7, 2011.
- [28] "JDSU Introduces Industry's Most Robust 100 Gigabit Ethernet Test Suite" (<http://www.jdsu.com/news/news-releases/2009/081909.html>). *News release.* JDS Uniphase. August 19, 2009. . Retrieved June 7, 2011.
- [29] "40/100 GbE: Testing the next generation of high speed Ethernet" (<http://www.spirent.com/Broadband/40-100G.aspx>). *commercial web site.* Spirent Communications. . Retrieved June 7, 2011.
- [30] "EXFO and Opnext Achieve Full Interoperability, Successfully Testing IEEE-Compliant 100 Gigabit Ethernet Optics" (<http://www.exfo.com/en/PressRoom/CorporateReleasesView.aspx?Id=453>). *News release.* January 11, 2010. . Retrieved June 7, 2011.
- [31] "Workshop on 100 Gigabit Ethernet a huge success" ([http://www.dtu.dk/English/About\\_DTU/News.aspx?guid={4518DC72-CA94-4D28-BB45-F7627FE581AA}](http://www.dtu.dk/English/About_DTU/News.aspx?guid={4518DC72-CA94-4D28-BB45-F7627FE581AA})). *DTU news* (Technical University of Denmark). February 2, 2011. . Retrieved June 7, 2011.
- [32] Torben R. Simonsen (January 26, 2011). "Dansk virksomhed klar med test til 100 Gb ethernet" (<http://elektronikbranchen.dk/nyhed/dansk-virksomhed-klar-med-test-til-100-gb-ethernet>). *Elektronik Branchen*. . Retrieved June 7, 2011. (Danish)
- [33] 100G in routers (<http://conference.vde.com/ecoc-2009/programs/documents/ecoc09-100g-ws-juniper-ceuppens.pdf>) Juniper Networks Presentation at ECOC 2009
- [34] "Huawei's 100G is out of the door" ([http://www.lightreading.com/document.asp?doc\\_id=209530](http://www.lightreading.com/document.asp?doc_id=209530)). .
- [35] "Alcatel-Lucent unveils industry-leading 100G IP technology in China" ([http://www.lightreading.com/top-picks.asp?doc\\_id=180764](http://www.lightreading.com/top-picks.asp?doc_id=180764)). .
- [36] "OPTICS UPDATE April 2011" ([http://www.alcatel.ru/wps/DocumentStreamerServlet?LMSG\\_CABINET=Docs\\_and\\_Resource\\_Ctr&LMSG\\_CONTENT\\_FILE=Financial\\_Info/Fin\\_Releases/IR-Financial\\_Analysts\\_Optics\\_april-1st-2011.pdf](http://www.alcatel.ru/wps/DocumentStreamerServlet?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=Financial_Info/Fin_Releases/IR-Financial_Analysts_Optics_april-1st-2011.pdf)). .
- [37] "Verizon completes industry-leading 100G Ethernet field trial" ([http://www.alcatel-lucent.com/wps/portal/!ut/p/kcxml/04\\_Sj9SPykssy0xPLMnMz0vM0Y\\_QjzKLd4w3MfQFSYGYRq6m-pEoYgbxjgiRIH1vfV-P\\_NxU\\_QD9gtzQiHJHR0UAAD\\_zXg!!/delta/base64xml/L0lJayEvUUd3QndJQSEvNEIVRkNBISEvNI9BX0U4QS9lb93dw!!?LMSG\\_CABINET=Docs\\_and\\_Resource\\_Ctr&LMSG\\_CONTENT\\_FILE=News\\_Releases\\_2010/News\\_Article\\_002116.xml](http://www.alcatel-lucent.com/wps/portal/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4w3MfQFSYGYRq6m-pEoYgbxjgiRIH1vfV-P_NxU_QD9gtzQiHJHR0UAAD_zXg!!/delta/base64xml/L0lJayEvUUd3QndJQSEvNEIVRkNBISEvNI9BX0U4QS9lb93dw!!?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=News_Releases_2010/News_Article_002116.xml)). .
- [38] "Alcatel-Lucent's FP3 network processor routes at 400Gbps" (<http://www.engadget.com/2011/06/29/alcatel-lucents-fp3-network-processor-routes-at-400mbps-handle/>). .
- [39] "Alcatel-Lucent and P&TLuxembourg launch one of Europe's fastest data networks" ([http://www.alcatel-lucent.com/wps/portal/!ut/p/kcxml/04\\_Sj9SPykssy0xPLMnMz0vM0Y\\_QjzKLd4w3MfQFSYGYRq6m-pEoYgbxjgiRIH1vfV-P\\_NxU\\_QD9gtzQiHJHR0UAAD\\_zXg!!/](http://www.alcatel-lucent.com/wps/portal/!ut/p/kcxml/04_Sj9SPykssy0xPLMnMz0vM0Y_QjzKLd4w3MfQFSYGYRq6m-pEoYgbxjgiRIH1vfV-P_NxU_QD9gtzQiHJHR0UAAD_zXg!!/)

- delta/base64xml/L0IJayEvUUd3QndJQSEvNEIVRkNBISEvNl9BX0U4QS9lbI93dw!!?LMSG\_CABINET=Docs\_and\_Resource\_Ctr&LMSG\_CONTENT\_FILE=News\_Releases\_2011/News\_Article\_002507.xml)..
- [40] "P&TLuxembourg employs Alcatel-Lucent for 100G optical, Ethernet network" (<http://www.carrierethernetnews.com/articles/300299/plluxembourg-employs-alcatel-lucent-for-100g-optic/>)..
- [41] "Alcatel-Lucent. P&TLuxembourg pair for 100-Gbps IP link" (<http://www.lightwaveonline.com/articles/2011/09/alcatel-lucent-plluxembourg-pair-for-100-gbps-ip-link-130132098.html>)..
- [42] Brocade set to unveil 100G Ethernet (<http://www.networkworld.com/news/2010/090110-brocade.html>) Brocade
- [43] "3 new services are launched by AMS-IX at MORE IP event" (<http://www.ams-ix.net/3-new-services-are-launched-by-ams-ix-at-more-ip-event/>)..
- [44] "Cisco NGN Transport Solutions" ([http://www.cisco.com/web/EA/expomorocco2009/docs/cisco\\_Expo\\_2009\\_NGN\\_Transport\\_published.pdf](http://www.cisco.com/web/EA/expomorocco2009/docs/cisco_Expo_2009_NGN_Transport_published.pdf))..
- [45] Matsumoto, Craig (April 11, 2011). "AT&T, Comcast Go Live With 100G" ([http://www.lightreading.com/document.asp?doc\\_id=206615&site=lr\\_cable](http://www.lightreading.com/document.asp?doc_id=206615&site=lr_cable)). Light Reading. . Retrieved December 17, 2011.
- [46] Liu, Stephen (July 25, 2011). "Cisco Live! Showing Off 100GbE on CRS-3 and ASR 9000 Series" (<http://blogs.cisco.com/sp/cisco-live-showing-off-100ge-on-crs-3-and-asr-9000-series/>). blogs.cisco.com. . Retrieved December 17, 2011.
- [47] "Huawei Successfully Develops 100 Gigabit Ethernet WDM Prototype" ([http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-076816-corporate-2-optical-dwdmbackbone-transport\\_network.htm](http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-076816-corporate-2-optical-dwdmbackbone-transport_network.htm))..
- [48] "Huawei Launches World's First End-to-End 100G Solutions" (<http://www.huawei.com/en/about-huawei/newsroom/press-release/hw-062645-corporate-ran-wnm-ran-wnp-ds-wisg-vs-win.htm>)..
- [49] "Huawei E2E 100G Solution" (<http://www.huawei.com/en/static/hw-076756.pdf>)..
- [50] "Russia's MegaFon Awards Backbone Contract to Huawei" (<http://www.cellular-news.com/story/45839.php>). .
- [51] "Huawei Unveils the World's First 200G High-Speed Line Card for Routers" (<http://www.huawei.com/ilink/en/about-huawei/newsroom/press-release/092592?KeyTemps=200G,Router>). .
- [52] "Huawei 200G Solution" ([http://www.huawei.com/ilink/en/solutions/expand-broadband/HW\\_092902?KeyTemps=#](http://www.huawei.com/ilink/en/solutions/expand-broadband/HW_092902?KeyTemps=#)). .
- [53] "Оборудование Huawei 100G успешно прошло тестирование в России" (<http://www.huawei.com/ru/catalog.do?id=4630>). .
- [54] "Juniper networks introduces breakthrough 100 gigabit ethernet interface for t series routers" ([http://www.juniper.net/us/en/company/press-center/press-releases/2009/pr\\_2009\\_06\\_08-09\\_00.html](http://www.juniper.net/us/en/company/press-center/press-releases/2009/pr_2009_06_08-09_00.html)). .
- [55] "Internet2 racing ahead with 100G Ethernet network" (<http://www.networkworld.com/community/blog/internet2-racing-ahead-100g-ethernet-network>). .
- [56] "Juniper Demonstrates Industry's First Live 100G Traffic From the Network Core to Edge" (<http://investor.juniper.net/phoenix.zhtml?c=69801&p=irol-newsArticle&ID=1496199&highlight=..>)..
- [57] "Verizon First Service Provider to Announce 100G Deployment on U.S. Network" (<http://www.verizonbusiness.com/about/news/pr-25717-en-Verizon+First+Service+Provider+to+Announce+100G+Deployment+on+U.S.+Network.xml>)..
- [58] Deploying 100GE (<http://www.uknof.org.uk/uknof19/Evans-Deploying-100Ge.pdf>) JANET UK
- [59] "40Gb/s Ethernet Single-mode Fibre PMD Study Group" (<http://www.ieee802.org/3/40GSMF/index.html>). *official web site*. IEEE 802. February 1, 2010. . Retrieved June 7, 2011.
- [60] "IEEE 802.3ba standard released" (<http://www.net-security.org/secworld.php?id=9448>). *Help Net Security web site*. June 21, 2010. . Retrieved June 24, 2011. "The IEEE 802.3ba standard, ratified June 17, 2010, ..." .
- [61] Ilango Ganga (September 21, 2009). "Chief Editor's Report" ([http://www.ieee802.org/3/ba/public/sep09/ganga\\_01\\_0909.pdf](http://www.ieee802.org/3/ba/public/sep09/ganga_01_0909.pdf)). *IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force public record. Archived* (<http://www.webcitation.org/5k77zk14S>) from the original on September 27, 2009. . Retrieved June 7, 2011.

## Further reading

- Overview of Requirements and Applications for 40 Gigabit Ethernet and 100 Gigabit Ethernet Technology Overview White Paper ([http://www.ethernetalliance.org/files/static\\_page\\_files/D13DCE87-1D09-3519-AD13E838D3CB0181/126\\_OVERVIEW\\_AND\\_APPLICATIONS2.pdf](http://www.ethernetalliance.org/files/static_page_files/D13DCE87-1D09-3519-AD13E838D3CB0181/126_OVERVIEW_AND_APPLICATIONS2.pdf)) ( Archived (<http://www.webcitation.org/5iiKRuVcu>) 2009-08-01) – Ethernet Alliance
- 40 Gigabit Ethernet and 100 Gigabit Ethernet Technology Overview White Paper ([http://www.ethernetalliance.org/wp-content/uploads/2011/10/document\\_files\\_40G\\_100G\\_Tech\\_overview.pdf](http://www.ethernetalliance.org/wp-content/uploads/2011/10/document_files_40G_100G_Tech_overview.pdf)) – Ethernet Alliance

## External links

- IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force (<http://www.ieee802.org/3/ba/public/index.html>)
- Ethernet Alliance (<http://www.ethernetalliance.org>)
- "100G Ethernet cheat sheet: A collection of articles, slideshows, multimedia content on 100G Ethernet" (<http://www.networkworld.com/news/2009/111909-100g-ethernet-cheatsheet.html>). *Network World*. November 19, 2009. Retrieved June 7, 2011.

# Standards

## IP address

An **Internet Protocol address (IP address)** is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.<sup>[1]</sup> An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."<sup>[2]</sup>

The designers of the Internet Protocol defined an IP address as a 32-bit number<sup>[1]</sup> and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995.<sup>[3]</sup> IPv6 was standardized as RFC 2460 in 1998,<sup>[4]</sup> and its deployment has been ongoing since the mid-2000s.

IP addresses are binary numbers, but they are usually stored in text files and displayed in human-readable notations, such as 172.16.254.1 (for IPv4), and 2001:db8:0:1234:0:567:8:1 (for IPv6).

The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally and delegates five regional Internet registries (RIRs) to allocate IP address blocks to local Internet registries (Internet service providers) and other entities.

## IP versions

Two versions of the Internet Protocol (IP) are in use: IP Version 4 and IP Version 6. Each version defines an IP address differently. Because of its prevalence, the generic term *IP address* typically still refers to the addresses defined by IPv4. The gap in version sequence between IPv4 and IPv6 resulted from the assignment of number 5 to the experimental Internet Stream Protocol in 1979, which however was never referred to as IPv5.

### IPv4 addresses

In IPv4 an address consists of 32 bits which limits the address space to 4294967296 ( $2^{32}$ ) possible unique addresses. IPv4 reserves some addresses for special purposes such as private networks (~18 million addresses) or multicast addresses (~270 million addresses).

IPv4 addresses are canonically represented in dot-decimal notation, which consists of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 172.16.254.1. Each part represents a group of 8 bits (octet) of the address. In some cases of technical writing, IPv4 addresses may be presented in various hexadecimal, octal, or binary representations.

#### An IPv4 address (dotted-decimal notation)

**172 . 16 . 254 . 1**



10101100 . 00010000 . 11111110 . 00000001

One byte = Eight bits

Thirty-two bits (4 x 8), or 4 bytes

Decomposition of an IPv4 address from dot-decimal notation to its binary value.

## IPv4 subnetting

In the early stages of development of the Internet Protocol,<sup>[1]</sup> network administrators interpreted an IP address in two parts: network number portion and host number portion. The highest order octet (most significant eight bits) in an address was designated as the *network number* and the remaining bits were called the *rest field* or *host identifier* and were used for host numbering within a network.

This early method soon proved inadequate as additional networks developed that were independent of the existing networks already designated by a network number. In 1981, the Internet addressing specification was revised with the introduction of classful network architecture.<sup>[2]</sup>

Classful network design allowed for a larger number of individual network assignments and fine-grained subnetwork design. The first three bits of the most significant octet of an IP address were defined as the *class* of the address. Three classes (*A*, *B*, and *C*) were defined for universal unicast addressing. Depending on the class derived, the network identification was based on octet boundary segments of the entire address. Each class used successively additional octets in the network identifier, thus reducing the possible number of hosts in the higher order classes (*B* and *C*). The following table gives an overview of this now obsolete system.

Class	Leading bits in address (binary)	Range of first octet (decimal)	Network ID format	Host ID format	Number of networks	Number of addresses per network
<b>A</b>	0	0–127	a	b.c.d	$2^7 = 128$	$2^{24} = 16777216$
<b>B</b>	10	128–191	a.b	c.d	$2^{14} = 16384$	$2^{16} = 65536$
<b>C</b>	110	192–223	a.b.c	d	$2^{21} = 2097152$	$2^8 = 256$

### + Historical classful network architecture

Classful network design served its purpose in the startup stage of the Internet, but it lacked scalability in the face of the rapid expansion of the network in the 1990s. The class system of the address space was replaced with Classless Inter-Domain Routing (CIDR) in 1993. CIDR is based on variable-length subnet masking (VLSM) to allow allocation and routing based on arbitrary-length prefixes.

Today, remnants of classful network concepts function only in a limited scope as the default configuration parameters of some network software and hardware components (e.g. netmask), and in the technical jargon used in network administrators' discussions.

## IPv4 private addresses

Early network design, when global end-to-end connectivity was envisioned for communications with all Internet hosts, intended that IP addresses be uniquely assigned to a particular computer or device. However, it was found that this was not always necessary as private networks developed and public address space needed to be conserved.

Computers not connected to the Internet, such as factory machines that communicate only with each other via TCP/IP, need not have globally unique IP addresses. Three ranges of IPv4 addresses for private networks were reserved in RFC 1918. These addresses are not routed on the Internet and thus their use need not be coordinated with an IP address registry.

Today, when needed, such private networks typically connect to the Internet through network address translation (NAT).

## IANA-reserved private IPv4 network ranges

	Start	End	No. of addresses
24-bit block (/8 prefix, 1 × A)	10.0.0.0	10.255.255.255	16777216
20-bit block (/12 prefix, 16 × B)	172.16.0.0	172.31.255.255	1048576
16-bit block (/16 prefix, 256 × C)	192.168.0.0	192.168.255.255	65536

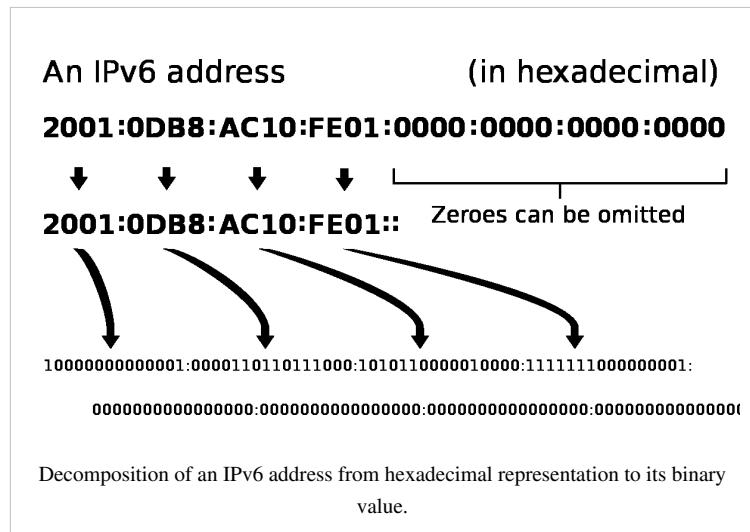
Any user may use any of the reserved blocks. Typically, a network administrator will divide a block into subnets; for example, many home routers automatically use a default address range of 192.168.0.0 through 192.168.0.255 (192.168.0.0/24).

## IPv4 address exhaustion

IPv4 address exhaustion is the decreasing supply of unallocated Internet Protocol Version 4 (IPv4) addresses available at the Internet Assigned Numbers Authority (IANA) and the regional Internet registries (RIRs) for assignment to end users and local Internet registries, such as Internet service providers. IANA's primary address pool was exhausted on 3 February 2011, when the last 5 blocks were allocated to the 5 RIRs.<sup>[5][6]</sup> APNIC was the first RIR to exhaust its regional pool on 15 April 2011, except for a small amount of address space reserved for the transition to IPv6, intended to be allocated in a restricted process.<sup>[7]</sup>

## IPv6 addresses

The rapid exhaustion of IPv4 address space, despite conservation techniques, prompted the Internet Engineering Task Force (IETF) to explore new technologies to expand the Internet's addressing capability. The permanent solution was deemed to be a redesign of the Internet Protocol itself. This next generation of the Internet Protocol, intended to replace IPv4 on the Internet, was eventually named *Internet Protocol Version 6* (IPv6) in 1995.<sup>[3][4]</sup> The address size was increased from 32 to 128 bits or 16 octets. This, even with a generous assignment of network blocks, is deemed sufficient for the foreseeable future. Mathematically, the new address space provides the potential for a maximum of  $2^{128}$ , or about  $3.403 \times 10^{38}$  unique addresses.



The new design is not intended to provide a sufficient quantity of addresses on its own, but rather to allow efficient aggregation of subnet routing prefixes to occur at routing nodes. As a result, routing table sizes are smaller, and the smallest possible individual allocation is a subnet for  $2^{64}$  hosts, which is the square of the size of the entire IPv4 Internet. At these levels, actual address utilization rates will be small on any IPv6 network segment. The new design also provides the opportunity to separate the addressing infrastructure of a network segment — that is the local administration of the segment's available space — from the addressing prefix used to route external traffic for a network. IPv6 has facilities that automatically change the routing prefix of entire networks, should the global connectivity or the routing policy change, without requiring internal redesign or renumbering.

The large number of IPv6 addresses allows large blocks to be assigned for specific purposes and, where appropriate, to be aggregated for efficient routing. With a large address space, there is not the need to have complex address

conservation methods as used in Classless Inter-Domain Routing (CIDR).

Many modern desktop and enterprise server operating systems include native support for the IPv6 protocol, but it is not yet widely deployed in other devices, such as home networking routers, voice over IP (VoIP) and multimedia equipment, and network peripherals.

### IPv6 private addresses

Just as IPv4 reserves addresses for private or internal networks, blocks of addresses are set aside in IPv6 for private addresses. In IPv6, these are referred to as unique local addresses (ULA). RFC 4193 sets aside the routing prefix fc00::/7 for this block which is divided into two /8 blocks with different implied policies. The addresses include a 40-bit pseudorandom number that minimizes the risk of address collisions if sites merge or packets are misrouted.<sup>[8]</sup>

Early designs used a different block for this purpose (fec0::), dubbed site-local addresses.<sup>[9]</sup> However, the definition of what constituted *sites* remained unclear and the poorly defined addressing policy created ambiguities for routing. This address range specification was abandoned and must not be used in new systems.<sup>[10]</sup>

Addresses starting with fe80:, called link-local addresses, are assigned to interfaces for communication on the link only. The addresses are automatically generated by the operating system for each network interface. This provides instant and automatic network connectivity for any IPv6 host and means that if several hosts connect to a common hub or switch, they have a communication path via their link-local IPv6 address. This feature is used in the lower layers of IPv6 network administration (e.g. Neighbor Discovery Protocol).

None of the private address prefixes may be routed on the public Internet.

## IP subnetworks

IP networks may be divided into subnetworks in both IPv4 and IPv6. For this purpose, an IP address is logically recognized as consisting of two parts: the *network prefix* and the *host identifier*, or *interface identifier* (IPv6). The subnet mask or the CIDR prefix determines how the IP address is divided into network and host parts.

The term *subnet mask* is only used within IPv4. Both IP versions however use the Classless Inter-Domain Routing (CIDR) concept and notation. In this, the IP address is followed by a slash and the number (in decimal) of bits used for the network part, also called the *routing prefix*. For example, an IPv4 address and its subnet mask may be 192.0.2.1 and 255.255.255.0, respectively. The CIDR notation for the same IP address and subnet is 192.0.2.1/24, because the first 24 bits of the IP address indicate the network and subnet.

## IP address assignment

Internet Protocol addresses are assigned to a host either anew at the time of booting, or permanently by fixed configuration of its hardware or software. Persistent configuration is also known as using a *static IP address*. In contrast, in situations when the computer's IP address is assigned newly each time, this is known as using a *dynamic IP address*.

### Methods

Static IP addresses are manually assigned to a computer by an administrator. The exact procedure varies according to platform. This contrasts with dynamic IP addresses, which are assigned either by the computer interface or host software itself, as in Zeroconf, or assigned by a server using Dynamic Host Configuration Protocol (DHCP). Even though IP addresses assigned using DHCP may stay the same for long periods of time, they can generally change. In some cases, a network administrator may implement dynamically assigned static IP addresses. In this case, a DHCP server is used, but it is specifically configured to always assign the same IP address to a particular computer. This allows static IP addresses to be configured centrally, without having to specifically configure each computer on the network in a manual procedure.

In the absence or failure of static or stateful (DHCP) address configurations, an operating system may assign an IP address to a network interface using state-less auto-configuration methods, such as Zeroconf.

## Uses of dynamic addressing

Dynamic IP addresses are most frequently assigned on LANs and broadband networks by Dynamic Host Configuration Protocol (DHCP) servers. They are used because it avoids the administrative burden of assigning specific static addresses to each device on a network. It also allows many devices to share limited address space on a network if only some of them will be online at a particular time. In most current desktop operating systems, dynamic IP configuration is enabled by default so that a user does not need to manually enter any settings to connect to a network with a DHCP server. DHCP is not the only technology used to assign dynamic IP addresses. Dialup and some broadband networks use dynamic address features of the Point-to-Point Protocol.

### Sticky dynamic IP address

A *sticky dynamic IP address* is an informal term used by cable and DSL Internet access subscribers to describe a dynamically assigned IP address which seldom changes. The addresses are usually assigned with DHCP. Since the modems are usually powered on for extended periods of time, the address leases are usually set to long periods and simply renewed. If a modem is turned off and powered up again before the next expiration of the address lease, it will most likely receive the same IP address.

## Address autoconfiguration

RFC 3330 defines an address block, 169.254.0.0/16, for the special use in link-local addressing for IPv4 networks. In IPv6, every interface, whether using static or dynamic address assignments, also receives a local-link address automatically in the block fe80::/10.

These addresses are only valid on the link, such as a local network segment or point-to-point connection, that a host is connected to. These addresses are not routable and like private addresses cannot be the source or destination of packets traversing the Internet.

When the link-local IPv4 address block was reserved, no standards existed for mechanisms of address autoconfiguration. Filling the void, Microsoft created an implementation that is called Automatic Private IP Addressing (APIPA). Due to Microsoft's market power, APIPA has been deployed on millions of machines and has, thus, become a de facto standard in the industry. Many years later, the IETF defined a formal standard for this functionality, RFC 3927, entitled *Dynamic Configuration of IPv4 Link-Local Addresses*.

## Uses of static addressing

Some infrastructure situations have to use static addressing, such as when finding the Domain Name System (DNS) host that will translate domain names to IP addresses. Static addresses are also convenient, but not absolutely necessary, to locate servers inside an enterprise. An address obtained from a DNS server comes with a time to live, or caching time, after which it should be looked up to confirm that it has not changed. Even static IP addresses do change as a result of network administration (RFC 2072).

## Public addresses

A *public IP address*, in common parlance, is synonymous with a *globally routable unicast IP address*.

Both IPv4 and IPv6 define address ranges that are reserved for private networks and link-local addressing. The term public IP address often used excludes these types of addresses.

## Modifications to IP addressing

### IP blocking and firewalls

Firewalls perform Internet Protocol blocking to protect networks from unauthorized access. They are common on today's Internet. They control access to networks based on the IP address of a client computer. Whether using a blacklist or a whitelist, the IP address that is blocked is the perceived IP address of the client, meaning that if the client is using a proxy server or network address translation, blocking one IP address may block many individual computers.

### IP address translation

Multiple client devices can appear to share IP addresses: either because they are part of a shared hosting web server environment or because an IPv4 network address translator (NAT) or proxy server acts as an intermediary agent on behalf of its customers, in which case the real originating IP addresses might be hidden from the server receiving a request. A common practice is to have a NAT hide a large number of IP addresses in a private network. Only the "outside" interface(s) of the NAT need to have Internet-routable addresses.<sup>[11]</sup>

Most commonly, the NAT device maps TCP or UDP port numbers on the outside to individual private addresses on the inside. Just as a telephone number may have site-specific extensions, the port numbers are site-specific extensions to an IP address.

In small home networks, NAT functions usually take place in a residential gateway device, typically one marketed as a "router". In this scenario, the computers connected to the router would have 'private' IP addresses and the router would have a 'public' address to communicate with the Internet. This type of router allows several computers to share one public IP address.

## Diagnostic tools

Computer operating systems provide various diagnostic tools to examine their network interface and address configuration. Windows provides the command-line interface tools `ipconfig` and `netsh` and users of Unix-like systems can use `ifconfig`, `netstat`, `route`, `lanstat`, `ifstat`, or `iproute2` utilities to accomplish the task.

## References

- [1] RFC 760, *DOD Standard Internet Protocol* (January 1980)
- [2] RFC 791, *Internet Protocol - DARPA Internet Program Protocol Specification* (September 1981)
- [3] RFC 1883, *Internet Protocol, Version 6 (IPv6) Specification*, S. Deering, R. Hinden (December 1995)
- [4] RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, S. Deering, R. Hinden, The Internet Society (December 1998)
- [5] Smith, Lucie; Lipner, Ian (3 February 2011). "Free Pool of IPv4 Address Space Depleted" (<http://www.nro.net/news/ipv4-free-pool-depleted>). Number Resource Organization. . Retrieved 3 February 2011.
- [6] ICANN,nanog mailing list. "Five /8s allocated to RIRs - no unallocated IPv4 unicast /8s remain" (<http://mailman.nanog.org/pipermail/nanog/2011-February/032107.html>). .
- [7] Asia-Pacific Network Information Centre (15 April 2011). "APNIC IPv4 Address Pool Reaches Final /8" (<http://www.apnic.net/publications/news/2011/final-8>). . Retrieved 15 April 2011.
- [8] RFC 4193 section 3.2.1
- [9] RFC 3513

- [10] RFC 3879
- [11] Comer, Douglas (2000). *Internetworking with TCP/IP: Principles, Protocols, and Architectures -- 4th ed.* (<http://www.cs.purdue.edu/homes/dec/netbooks.html>). Upper Saddle River, NJ: Prentice Hall. p. 394. ISBN 0-13-018380-6. .

## External links

- IP (<http://www.dmoz.org/Computers/Internet/Protocols/IP/>) at the Open Directory Project
- "Understanding IP Addressing: Everything You Ever Wanted To Know" ([http://web.archive.org/web/20100821112028/http://www.3com.com/other/pdfs/infra/corpinfo/en\\_US/501302.pdf](http://web.archive.org/web/20100821112028/http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf)). Archived from the original ([http://www.3com.com/other/pdfs/infra/corpinfo/en\\_US/501302.pdf](http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf)) on 21 August 2010.

# Transmission Control Protocol

---

The **Transmission Control Protocol (TCP)** is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite, complementing the Internet Protocol (IP), and therefore the entire suite is commonly referred to as *TCP/IP*. TCP provides reliable, ordered delivery of a stream of octets from a program on one computer to another program on another computer. TCP is the protocol used by major Internet applications such as the World Wide Web, email, remote administration and file transfer. Other applications, which do not require reliable data stream service, may use the User Datagram Protocol (UDP), which provides a datagram service that emphasizes reduced latency over reliability.

## Historical origin

In May 1974 the Institute of Electrical and Electronic Engineers (IEEE) published a paper entitled "*A Protocol for Packet Network Intercommunication*."<sup>[1]</sup> The paper's authors, Vint Cerf and Bob Kahn, described an internetworking protocol for sharing resources using packet-switching among the nodes. A central control component of this model was the *Transmission Control Program* that incorporated both connection-oriented links and datagram services between hosts. The monolithic Transmission Control Program was later divided into a modular architecture consisting of the *Transmission Control Protocol* at the connection-oriented layer and the *Internet Protocol* at the internetworking (datagram) layer. The model became known informally as *TCP/IP*, although formally it was henceforth called the *Internet Protocol Suite*.

## Network function

The protocol corresponds to the transport layer of TCP/IP suite. TCP provides a communication service at an intermediate level between an application program and the Internet Protocol (IP). That is, when an application program desires to send a large chunk of data across the Internet using IP, instead of breaking the data into IP-sized pieces and issuing a series of IP requests, the software can issue a single request to TCP and let TCP handle the IP details.

IP works by exchanging pieces of information called packets. A packet is a sequence of octets and consists of a *header* followed by a *body*. The header describes the packet's destination and, optionally, the routers to use for forwarding until it arrives at its destination. The body contains the data IP is transmitting.

Due to network congestion, traffic load balancing, or other unpredictable network behavior, IP packets can be lost, duplicated, or delivered out of order. TCP detects these problems, requests retransmission of lost data, rearranges out-of-order data, and even helps minimize network congestion to reduce the occurrence of the other problems. Once the TCP receiver has reassembled the sequence of octets originally transmitted, it passes them to the application program. Thus, TCP abstracts the application's communication from the underlying networking details.

TCP is utilized extensively by many of the Internet's most popular applications, including the World Wide Web (WWW), E-mail, File Transfer Protocol, Secure Shell, peer-to-peer file sharing, and some streaming media applications.

TCP is optimized for accurate delivery rather than timely delivery, and therefore, TCP sometimes incurs relatively long delays (in the order of seconds) while waiting for out-of-order messages or retransmissions of lost messages. It is not particularly suitable for real-time applications such as Voice over IP. For such applications, protocols like the Real-time Transport Protocol (RTP) running over the User Datagram Protocol (UDP) are usually recommended instead.<sup>[2]</sup>

TCP is a reliable stream delivery service that guarantees that all bytes received will be identical with bytes sent and in the correct order. Since packet transfer is not reliable, a technique known as positive acknowledgment with retransmission is used to guarantee reliability of packet transfers. This fundamental technique requires the receiver to respond with an acknowledgment message as it receives the data. The sender keeps a record of each packet it sends. The sender also keeps a timer from when the packet was sent, and retransmits a packet if the timer expires before the message has been acknowledged. The timer is needed in case a packet gets lost or corrupted.<sup>[2]</sup>

TCP consists of a set of rules: for the protocol, that are used with the Internet Protocol, and for the IP, to send data "in a form of message units" between computers over the Internet. While IP handles actual delivery of the data, TCP keeps track of the individual units of data transmission, called *segments*, that a message is divided into for efficient routing through the network. For example, when an HTML file is sent from a Web server, the TCP software layer of that server divides the sequence of octets of the file into segments and forwards them individually to the IP software layer (Internet Layer). The Internet Layer encapsulates each TCP segment into an IP packet by adding a header that includes (among other data) the destination IP address. Even though every packet has the same destination address, they can be routed on different paths through the network. When the client program on the destination computer receives them, the TCP layer (Transport Layer) reassembles the individual segments and ensures they are correctly ordered and error free as it streams them to an application.

## TCP segment structure

Transmission Control Protocol accepts data from a data stream, segments it into chunks, and adds a TCP header creating a TCP segment. The TCP segment is then encapsulated into an Internet Protocol (IP) datagram. A TCP segment is "the packet of information that TCP uses to exchange data with its peers."<sup>[3]</sup>

The term *TCP packet*, though sometimes informally used, is not in line with current terminology, where *segment* refers to the TCP PDU (Protocol Data Unit), *datagram*<sup>[4]</sup> to the IP PDU and *frame* to the data link layer PDU:

Processes transmit data by calling on the TCP and passing buffers of data as arguments. The TCP packages the data from these buffers into segments and calls on the internet module [e.g. IP] to transmit each segment to the destination TCP.<sup>[5]</sup>

A TCP segment consists of a segment *header* and a *data* section. The TCP header contains 10 mandatory fields, and an optional extension field (*Options*, orange background in table).

The data section follows the header. Its contents are the payload data carried for the application. The length of the data section is not specified in the TCP segment header. It can be calculated by subtracting the combined length of the TCP header and the encapsulating IP header from the total IP datagram length (specified in the IP header).

## TCP Header

Offsets	Octet	0				1				2				3																			
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port															Destination port																
4	32	Sequence number															Acknowledgment number (if ACK set)																
8	64	Acknowledgment number (if ACK set)															Window Size																
12	96	Data offset	Reserved	N	C	E	U	A	P	R	S	F	Window Size																				
		0 0 0		S W C R C S S Y I	R E G K H T N N																												
16	128	Checksum															Urgent pointer (if URG set)																
20	160	Options (if Data Offset > 5, padded at the end with "0" bytes if necessary)															...																
...	...	...															...																

- Source port (16 bits) – identifies the sending port
- Destination port (16 bits) – identifies the receiving port
- Sequence number (32 bits) – has a dual role:
  - If the SYN flag is set (1), then this is the initial sequence number. The sequence number of the actual first data byte and the acknowledged number in the corresponding ACK are then this sequence number plus 1.
  - If the SYN flag is clear (0), then this is the accumulated sequence number of the first data byte of this packet for the current session.
- Acknowledgment number (32 bits) – if the ACK flag is set then the value of this field is the next sequence number that the receiver is expecting. This acknowledges receipt of all prior bytes (if any). The first ACK sent by each end acknowledges the other end's initial sequence number itself, but no data.
- Data offset (4 bits) – specifies the size of the TCP header in 32-bit words. The minimum size header is 5 words and the maximum is 15 words thus giving the minimum size of 20 bytes and maximum of 60 bytes, allowing for up to 40 bytes of options in the header. This field gets its name from the fact that it is also the offset from the start of the TCP segment to the actual data.
- Reserved (3 bits) – for future use and should be set to zero
- Flags (9 bits) (aka Control bits) – contains 9 1-bit flags
  - NS (1 bit) – ECN-nonce concealment protection (added to header by RFC 3540).
  - CWR (1 bit) – Congestion Window Reduced (CWR) flag is set by the sending host to indicate that it received a TCP segment with the ECE flag set and had responded in congestion control mechanism (added to header by RFC 3168).
  - ECE (1 bit) – ECN-Echo indicates
    - If the SYN flag is set (1), that the TCP peer is ECN capable.
    - If the SYN flag is clear (0), that a packet with Congestion Experienced flag in IP header set is received during normal transmission (added to header by RFC 3168).
  - URG (1 bit) – indicates that the Urgent pointer field is significant
  - ACK (1 bit) – indicates that the Acknowledgment field is significant. All packets after the initial SYN packet sent by the client should have this flag set.
  - PSH (1 bit) – Push function. Asks to push the buffered data to the receiving application.
  - RST (1 bit) – Reset the connection
  - SYN (1 bit) – Synchronize sequence numbers. Only the first packet sent from each end should have this flag set. Some other flags change meaning based on this flag, and some are only valid for when it is set, and others when it is clear.

- FIN (1 bit) – No more data from sender
- Window size (16 bits) – the size of the *receive window*, which specifies the number of bytes (beyond the sequence number in the acknowledgment field) that the sender of this segment is currently willing to receive (*see Flow control and Window Scaling*)
- Checksum (16 bits) – The 16-bit checksum field is used for error-checking of the header and data
- Urgent pointer (16 bits) – if the URG flag is set, then this 16-bit field is an offset from the sequence number indicating the last urgent data byte
- Options (Variable 0–320 bits, divisible by 32) – The length of this field is determined by the data offset field. Options have up to three fields: Option-Kind (1 byte), Option-Length (1 byte), Option-Data (variable). The Option-Kind field indicates the type of option, and is the only field that is not optional. Depending on what kind of option we are dealing with, the next two fields may be set: the Option-Length field indicates the total length of the option, and the Option-Data field contains the value of the option, if applicable. For example, an Option-Kind byte of 0x01 indicates that this is a No-Op option used only for padding, and does not have an Option-Length or Option-Data byte following it. An Option-Kind byte of 0 is the End Of Options option, and is also only one byte. An Option-Kind byte of 0x02 indicates that this is the Maximum Segment Size option, and will be followed by a byte specifying the length of the MSS field (should be 0x04). Note that this length is the total length of the given options field, including Option-Kind and Option-Length bytes. So while the MSS value is typically expressed in two bytes, the length of the field will be 4 bytes (+2 bytes of kind and length). In short, an MSS option field with a value of 0x05B4 will show up as (0x02 0x04 0x05B4) in the TCP options section.
- Padding – The TCP header padding is used to ensure that the TCP header ends and data begins on a 32 bit boundary. The padding is composed of zeros.<sup>[6]</sup>

Some options may only be sent when SYN is set; they are indicated below as <sup>[SYN]</sup>. Option-Kind and standard lengths given as (Option-Kind, Option-Length).

- 0 (8 bits) – End of options list
- 1 (8 bits) – No operation (NOP, Padding) This may be used to align option fields on 32-bit boundaries for better performance.
- 2,4,SS (32 bits) – Maximum segment size (*see maximum segment size*) <sup>[SYN]</sup>
- 3,3,S (24 bits) – Window scale (*see window scaling for details*) <sup>[SYN]</sup><sup>[7]</sup>
- 4,2 (16 bits) – Selective Acknowledgement permitted. <sup>[SYN]</sup> (*See selective acknowledgments for details*)<sup>[8]</sup>
- 5,N,BBBB,EEEE,... (variable bits, N is either 10, 18, 26, or 34)- Selective ACKnowledgement (SACK)<sup>[9]</sup>  
These first two bytes are followed by a list of 1–4 blocks being selectively acknowledged, specified as 32-bit begin/end pointers.
- 8,10,TTTT,EEEE (80 bits)- Timestamp and echo of previous timestamp (*see TCP timestamps for details*)<sup>[10]</sup>
- 14,3,S (24 bits) – TCP Alternate Checksum Request. <sup>[SYN]</sup><sup>[11]</sup>
- 15,N,... (variable bits) – TCP Alternate Checksum Data.

(The remaining options are obsolete, experimental, not yet standardized, or unassigned)

## Protocol operation

TCP protocol operations may be divided into three phases. Connections must be properly established in a multi-step handshake process (*connection establishment*) before entering the *data transfer* phase. After data transmission is completed, the *connection termination* closes established virtual circuits and releases all allocated resources.

A TCP connection is managed by an operating system through a programming interface that represents the local end-point for communications, the *Internet socket*. During the lifetime of a TCP connection it undergoes a series of state changes:<sup>[13]</sup>

### LISTEN

In case of a server, waiting for a connection request from any remote client.

### SYN-SENT

waiting for the remote peer to send back a TCP segment with the SYN and ACK flags set. ('SYN-SENT' state is usually set by TCP clients)

### SYN-RECEIVED

waiting for the remote peer to send back an acknowledgment after having sent back a connection acknowledgment to the remote peer. ('SYN-RECEIVED' state is usually set by TCP servers)

### ESTABLISHED

The port is ready to receive/send data from/to the remote peer.

### FIN-WAIT-1

Indicated that the server is waiting for the application process on its end to signal that it is ready to close.

### FIN-WAIT-2

Indicates that the client is waiting for the server's fin segment (which indicates the server's application process is ready to close and the server is ready to initiate its side of the connection termination)

### CLOSE-WAIT

The server receives notice from the local application that it is done. The server sends its fin to the client.

### LAST-ACK

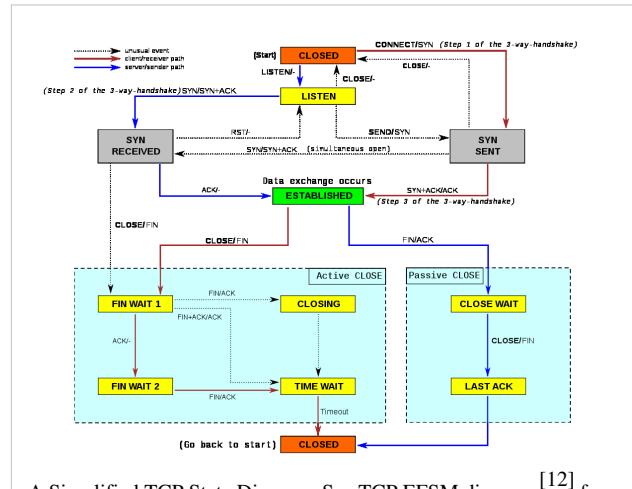
Indicates that the server is in the process of sending its own fin segment (which indicates the server's application process is ready to close and the server is ready to initiate its side of the connection termination )

### TIME-WAIT

Represents waiting for enough time to pass to be sure the remote peer received the acknowledgment of its connection termination request. According to RFC 793 a connection can stay in TIME-WAIT for a maximum of four minutes known as a MSL (maximum segment lifetime).

### CLOSED

Connection is closed



A Simplified TCP State Diagram. See TCP EFSM diagram [12] for a more detailed state diagram including the states inside the ESTABLISHED state.

## Connection establishment

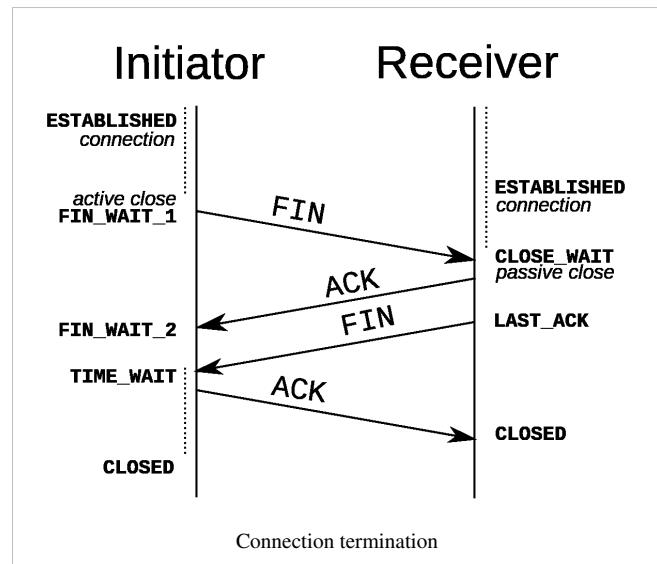
To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. To establish a connection, the three-way (or 3-step) handshake occurs:

1. **SYN**: The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.
2. **SYN-ACK**: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number ( $A + 1$ ), and the sequence number that the server chooses for the packet is another random number, B.
3. **ACK**: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e.  $A + 1$ , and the acknowledgement number is set to one more than the received sequence number i.e.  $B + 1$ .

At this point, both the client and server have received an acknowledgment of the connection.

## Connection termination

The connection termination phase uses, at most, a four-way handshake, with each side of the connection terminating independently. When an endpoint wishes to stop half of the connection, it transmits a FIN packet, which the other end acknowledges with an ACK. Therefore, a typical tear-down requires a pair of FIN and ACK segments from each TCP endpoint. After both FIN/ACK exchanges are concluded, the terminating side waits for a timeout before finally closing the connection, during which time the local port is unavailable for new connections; this prevents confusion due to delayed packets being delivered during subsequent connections.



A connection can be "half-open", in which case one side has terminated its end, but the other has not. The side that has terminated can no longer send any data into the connection, but the other side can. The terminating side should continue reading the data until the other side terminates as well.

It is also possible to terminate the connection by a 3-way handshake, when host A sends a FIN and host B replies with a FIN & ACK (merely combines 2 steps into one) and host A replies with an ACK.<sup>[14]</sup> This is perhaps the most common method.

It is possible for both hosts to send FINs simultaneously then both just have to ACK. This could possibly be considered a 2-way handshake since the FIN/ACK sequence is done in parallel for both directions.

Some host TCP stacks may implement a half-duplex close sequence, as Linux or HP-UX do. If such a host actively closes a connection but still has not read all the incoming data the stack already received from the link, this host sends a RST instead of a FIN (Section 4.2.2.13 in RFC 1122<sup>[15]</sup>). This allows a TCP application to be sure the remote application has read all the data the former sent—waiting the FIN from the remote side, when it actively closes the connection. However, the remote TCP stack cannot distinguish between a *Connection Aborting RST* and this *Data Loss RST*. Both cause the remote stack to throw away all the data it received, but that the application still

didn't read.

Some application protocols may violate the OSI model layers, using the TCP open/close handshaking for the application protocol open/close handshaking — these may find the RST problem on active close. As an example:

```
s = connect(remote);
send(s, data);
close(s);
```

For a usual program flow like above, a TCP/IP stack like that described above does not guarantee that all the data arrives to the other application.

## Resource usage

Most implementations allocate an entry in a table that maps a session to a running operating system process. Because TCP packets do not include a session identifier, both endpoints identify the session using the client's address and port. Whenever a packet is received, the TCP implementation must perform a lookup on this table to find the destination process.

The number of sessions in the server side is limited only by memory and can grow as new connections arrive, but the client must allocate a random port before sending the first SYN to the server. This port remains allocated during the whole conversation, and effectively limits the number of outgoing connections from each of the client's IP addresses. If an application fails to properly close unrequired connections, a client can run out of resources and become unable to establish new TCP connections, even from other applications.

Both endpoints must also allocate space for unacknowledged packets and received (but unread) data.

## Data transfer

There are a few key features that set TCP apart from User Datagram Protocol:

- Ordered data transfer — the destination host rearranges according to sequence number<sup>[2]</sup>
- Retransmission of lost packets — any cumulative stream not acknowledged is retransmitted<sup>[2]</sup>
- Error-free data transfer<sup>[16]</sup>
- Flow control — limits the rate a sender transfers data to guarantee reliable delivery. The receiver continually hints the sender on how much data can be received (controlled by the sliding window). When the receiving host's buffer fills, the next acknowledgment contains a 0 in the window size, to stop transfer and allow the data in the buffer to be processed.<sup>[2]</sup>
- Congestion control<sup>[2]</sup>

## Reliable transmission

TCP uses a *sequence number* to identify each byte of data. The sequence number identifies the order of the bytes sent from each computer so that the data can be reconstructed in order, regardless of any fragmentation, disordering, or packet loss that may occur during transmission. For every payload byte transmitted, the sequence number must be incremented. In the first two steps of the 3-way handshake, both computers exchange an initial sequence number (ISN). This number can be arbitrary, and should in fact be unpredictable to defend against TCP Sequence Prediction Attacks.

TCP primarily uses a *cumulative acknowledgment* scheme, where the receiver sends an acknowledgment signifying that the receiver has received all data preceding the acknowledged sequence number. The sender sets the sequence number field to the sequence number of the first payload byte in the segment's data field, and the receiver sends an acknowledgment specifying the sequence number of the next byte they expect to receive. For example, if a sending computer sends a packet containing four payload bytes with a sequence number field of 100, then the sequence numbers of the four payload bytes are 100, 101, 102 and 103. When this packet arrives at the receiving computer, it

would send back an acknowledgment number of 104 since that is the sequence number of the next byte it expects to receive in the next packet.

In addition to cumulative acknowledgments, TCP receivers can also send selective acknowledgments to provide further information.

If the sender infers that data has been lost in the network, it retransmits the data.

### Error detection

Sequence numbers and acknowledgments cover discarding duplicate packets, retransmission of lost packets, and ordered-data transfer. To assure correctness a checksum field is included (*see TCP segment structure for details on checksumming*).

The TCP checksum is a weak check by modern standards. Data Link Layers with high bit error rates may require additional link error correction/detection capabilities. The weak checksum is partially compensated for by the common use of a CRC or better integrity check at layer 2, below both TCP and IP, such as is used in PPP or the Ethernet frame. However, this does not mean that the 16-bit TCP checksum is redundant: remarkably, introduction of errors in packets between CRC-protected hops is common, but the end-to-end 16-bit TCP checksum catches most of these simple errors.<sup>[17]</sup> This is the end-to-end principle at work.

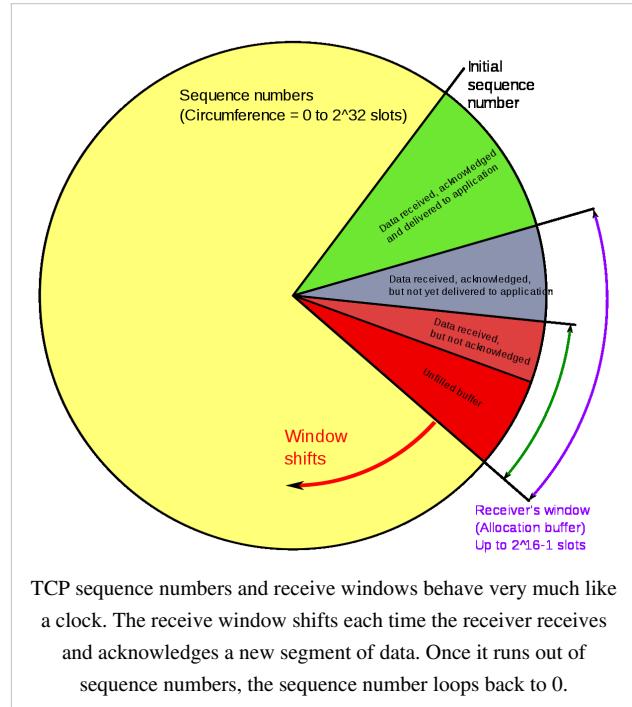
### Flow control

TCP uses an end-to-end flow control protocol to avoid having the sender send data too fast for the TCP receiver to receive and process it reliably. Having a mechanism for flow control is essential in an environment where machines of diverse network speeds communicate. For example, if a PC sends data to a smartphone that is slowly processing received data, the smartphone must regulate the data flow so as not to be overwhelmed.<sup>[2]</sup>

TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies in the *receive window* field the amount of additionally received data (in bytes) that it is willing to buffer for the connection. The sending host can send only up to that amount of data before it must wait for an acknowledgment and window update from the receiving host.

When a receiver advertises a window size of 0, the sender stops sending data and starts the *persist timer*. The persist timer is used to protect TCP from a deadlock situation that could arise if a subsequent window size update from the receiver is lost, and the sender cannot send more data until receiving a new window size update from the receiver. When the persist timer expires, the TCP sender attempts recovery by sending a small packet so that the receiver responds by sending another acknowledgement containing the new window size.

If a receiver is processing incoming data in small increments, it may repeatedly advertise a small receive window. This is referred to as the silly window syndrome, since it is inefficient to send only a few bytes of data in a TCP segment, given the relatively large overhead of the TCP header. TCP senders and receivers typically employ flow control logic to specifically avoid repeatedly sending small segments. The sender-side silly window syndrome avoidance logic is referred to as Nagle's algorithm.



### Congestion control

The final main aspect of TCP is congestion control. TCP uses a number of mechanisms to achieve high performance and avoid congestion collapse, where network performance can fall by several orders of magnitude. These mechanisms control the rate of data entering the network, keeping the data flow below a rate that would trigger collapse. They also yield an approximately max-min fair allocation between flows.

Acknowledgments for data sent, or lack of acknowledgments, are used by senders to infer network conditions between the TCP sender and receiver. Coupled with timers, TCP senders and receivers can alter the behavior of the flow of data. This is more generally referred to as congestion control and/or network congestion avoidance.

Modern implementations of TCP contain four intertwined algorithms: Slow-start, congestion avoidance, fast retransmit, and fast recovery (RFC 5681).

In addition, senders employ a *retransmission timeout* (RTO) that is based on the estimated round-trip time (or RTT) between the sender and receiver, as well as the variance in this round trip time. The behavior of this timer is specified in RFC 6298. There are subtleties in the estimation of RTT. For example, senders must be careful when calculating RTT samples for retransmitted packets; typically they use Karn's Algorithm or TCP timestamps (see RFC 1323). These individual RTT samples are then averaged over time to create a Smoothed Round Trip Time (SRTT) using Jacobson's algorithm. This SRTT value is what is finally used as the round-trip time estimate.

Enhancing TCP to reliably handle loss, minimize errors, manage congestion and go fast in very high-speed environments are ongoing areas of research and standards development. As a result, there are a number of TCP congestion avoidance algorithm variations.

### Maximum segment size

The maximum segment size (MSS) is the largest amount of data, specified in bytes, that TCP is willing to receive in a single segment. For best performance, the MSS should be set small enough to avoid IP fragmentation, which can lead to packet loss and excessive retransmissions. To try to accomplish this, typically the MSS is announced by each side using the MSS option when the TCP connection is established, in which case it is derived from the maximum transmission unit (MTU) size of the data link layer of the networks to which the sender and receiver are directly attached. Furthermore, TCP senders can use path MTU discovery to infer the minimum MTU along the network path between the sender and receiver, and use this to dynamically adjust the MSS to avoid IP fragmentation within the network.

MSS announcement is also often called "MSS negotiation". Strictly speaking, the MSS is not "negotiated" between the originator and the receiver, because that would imply that both originator and receiver will negotiate and agree upon a single, unified MSS that applies to all communication in both directions of the connection. In fact, two completely independent values of MSS are permitted for the two directions of data flow in a TCP connection.<sup>[18]</sup> This situation may arise, for example, if one of the devices participating in a connection has an extremely limited amount of memory reserved (perhaps even smaller than the overall discovered Path MTU) for processing incoming TCP segments.

### Selective acknowledgments

Relying purely on the cumulative acknowledgment scheme employed by the original TCP protocol can lead to inefficiencies when packets are lost. For example, suppose 10,000 bytes are sent in 10 different TCP packets, and the first packet is lost during transmission. In a pure cumulative acknowledgment protocol, the receiver cannot say that it received bytes 1,000 to 9,999 successfully, but failed to receive the first packet, containing bytes 0 to 999. Thus the sender may then have to resend all 10,000 bytes.

To solve this problem TCP employs the *selective acknowledgment (SACK)* option, defined in RFC 2018, which allows the receiver to acknowledge discontinuous blocks of packets that were received correctly, in addition to the

sequence number of the last contiguous byte received successively, as in the basic TCP acknowledgment. The acknowledgement can specify a number of *SACK blocks*, where each SACK block is conveyed by the starting and ending sequence numbers of a contiguous range that the receiver correctly received. In the example above, the receiver would send SACK with sequence numbers 1000 and 9999. The sender thus retransmits only the first packet, bytes 0 to 999.

An extension to the SACK option is the duplicate-SACK option, defined in RFC 2883. An out-of-order packet delivery can often falsely indicate the TCP sender of lost packet and, in turn, the TCP sender retransmits the suspected-to-be-lost packet and slow down the data delivery to prevent network congestion. The TCP sender undoes the action of slow-down, that is a recovery of the original pace of data transmission, upon receiving a D-SACK that indicates the retransmitted packet is duplicate.

The SACK option is not mandatory and it is used only if both parties support it. This is negotiated when connection is established. SACK uses the optional part of the TCP header (*see TCP segment structure for details*). The use of SACK is widespread — all popular TCP stacks support it. Selective acknowledgment is also used in Stream Control Transmission Protocol (SCTP).

## Window scaling

For more efficient use of high bandwidth networks, a larger TCP window size may be used. The TCP window size field controls the flow of data and its value is limited to between 2 and 65,535 bytes.

Since the size field cannot be expanded, a scaling factor is used. The TCP window scale option, as defined in RFC 1323, is an option used to increase the maximum window size from 65,535 bytes to 1 gigabyte. Scaling up to larger window sizes is a part of what is necessary for TCP Tuning.

The window scale option is used only during the TCP 3-way handshake. The window scale value represents the number of bits to left-shift the 16-bit window size field. The window scale value can be set from 0 (no shift) to 14 for each direction independently. Both sides must send the option in their SYN segments to enable window scaling in either direction.

Some routers and packet firewalls rewrite the window scaling factor during a transmission. This causes sending and receiving sides to assume different TCP window sizes. The result is non-stable traffic that may be very slow. The problem is visible on some sending and receiving sites behind the path of defective routers.<sup>[19]</sup>

## TCP timestamps

TCP timestamps, defined in RFC 1323, can help TCP determine in which order packets were sent. TCP timestamps are not normally aligned to the system clock and start at some random value. Many operating systems will increment the timestamp for every elapsed milisecond; however the RFC only states that the tics should be proportional.

There are two timestamp fields:

```
a 4-byte sender timestamp value (my timestamp)  
a 4-byte echo reply timestamp value (the most recent timestamp received from you).
```

TCP timestamps are used in an algorithm known as *Protection Against Wrapped Sequence* numbers, or PAWS (see RFC 1323 for details). PAWS is used when the TCP window size exceeds the possible numbers of sequence numbers ( $2^{32}$  or 4 billion/gig). In the case where a packet was potentially retransmitted it answers the question: "Is this sequence number in the first 4 GB or the second?" And the timestamp is used to break the tie.

RFC 1323 incorrectly states in section 2.2 that the window scale must be limited to  $2^{14}$  to remain under 1 GB (which is correct, but the sequence number limit is 4 GB); however a scale of 16 and a window size of 65535 would be 65536 less than the  $2^{32}$  possible sequence numbers and thus an acceptable yet excessive value. Because of this error many systems have limited the max scale to  $2^{14}$  to "follow the RFC".

Also, the Eifel detection algorithm (RFC 3522) uses TCP timestamps to determine if retransmissions are occurring because packets are lost or simply out of order.

## Out of band data

One is able to interrupt or abort the queued stream instead of waiting for the stream to finish. This is done by specifying the data as *urgent*. This tells the receiving program to process it immediately, along with the rest of the urgent data. When finished, TCP informs the application and resumes back to the stream queue. An example is when TCP is used for a remote login session, the user can send a keyboard sequence that interrupts or aborts the program at the other end. These signals are most often needed when a program on the remote machine fails to operate correctly. The signals must be sent without waiting for the program to finish its current transfer.<sup>[2]</sup>

TCP OOB data was not designed for the modern Internet. The *urgent* pointer only alters the processing on the remote host and doesn't expedite any processing on the network itself. When it gets to the remote host there are two slightly different interpretations of the protocol, which means only single bytes of OOB data are reliable. This is assuming it is reliable at all as it is one of the least commonly used protocol elements and tends to be poorly implemented.<sup>[20][21]</sup>

## Forcing data delivery

Normally, TCP waits for 200 ms or for a full packet of data to send (Nagle's Algorithm = tries to group small messages into a single packet). This creates minor, but potentially serious delays if repeated constantly during a file transfer. For example a typical send block would be 4 KB, a typical MSS is 1460, so 2 packets go out on a 10 Mbit/s ethernet taking ~1.2 ms each followed by a third carrying the remaining 1176 after a 197 ms pause because TCP is waiting for a full buffer.

In the case of telnet, each user keystroke is echoed back by the server before the user can see it on the screen. This delay would become very annoying.

Setting the socket option `TCP_NODELAY` overrides the default 200 ms send delay. Application programs use this socket option to force output to be sent after writing a character or line of characters.

The RFC defines the `PSH` push bit as "a message to the receiving TCP stack to send this data immediately up to the receiving application".<sup>[2]</sup> There is no way to indicate or control it in User space using Berkeley sockets and it is controlled by Protocol stack only.<sup>[22]</sup>

## Vulnerabilities

TCP may be attacked in a variety of ways. The results of a thorough security assessment of TCP, along with possible mitigations for the identified issues, was published in 2009,<sup>[23]</sup> and is currently being pursued within the IETF.<sup>[24]</sup>

## Denial of service

By using a spoofed IP address and repeatedly sending purposely assembled SYN packets, attackers can cause the server to consume large amounts of resources keeping track of the bogus connections. This is known as a SYN flood attack. Proposed solutions to this problem include SYN cookies and cryptographic puzzles. Sockstress is a similar attack, that might be mitigated with system resource management.<sup>[25]</sup> An advanced DoS attack involving the exploitation of the TCP Persist Timer was analyzed at Phrack #66.<sup>[26]</sup>

## Connection hijacking

An attacker who is able to eavesdrop a TCP session and redirect packets can hijack a TCP connection. To do so, the attacker learns the sequence number from the ongoing communication and forges a false segment that looks like the next segment in the stream. Such a simple hijack can result in one packet being erroneously accepted at one end. When the receiving host acknowledges the extra segment to the other side of the connection, synchronization is lost. Hijacking might be combined with ARP or routing attacks that allow taking control of the packet flow, so as to get permanent control of the hijacked TCP connection.<sup>[27]</sup>

Impersonating a different IP address was not difficult prior to RFC 1948, when the initial *sequence number* was easily guessable. That allowed an attacker to blindly send a sequence of packets that the receiver would believe to come from a different IP address, without the need to deploy ARP or routing attacks: it is enough to ensure that the legitimate host of the impersonated IP address is down, or bring it to that condition using denial of service attacks. This is why the initial sequence number is chosen at random.

## TCP ports

TCP uses port numbers to identify sending and receiving application end-points on a host, or *Internet sockets*. Each side of a TCP connection has an associated 16-bit unsigned port number (0-65535) reserved by the sending or receiving application. Arriving TCP data packets are identified as belonging to a specific TCP connection by its sockets, that is, the combination of source host address, source port, destination host address, and destination port. This means that a server computer can provide several clients with several services simultaneously, as long as a client takes care of initiating any simultaneous connections to one destination port from different source ports.

Port numbers are categorized into three basic categories: well-known, registered, and dynamic/private. The well-known ports are assigned by the Internet Assigned Numbers Authority (IANA) and are typically used by system-level or root processes. Well-known applications running as servers and passively listening for connections typically use these ports. Some examples include: FTP (20 and 21), SSH (22), TELNET (23), SMTP (25), SSL (443) and HTTP (80). Registered ports are typically used by end user applications as ephemeral source ports when contacting servers, but they can also identify named services that have been registered by a third party. Dynamic/private ports can also be used by end user applications, but are less commonly so. Dynamic/private ports do not contain any meaning outside of any particular TCP connection.

## Development

TCP is a complex protocol. However, while significant enhancements have been made and proposed over the years, its most basic operation has not changed significantly since its first specification RFC 675 in 1974, and the v4 specification RFC 793, published in September 1981. RFC 1122, Host Requirements for Internet Hosts, clarified a number of TCP protocol implementation requirements. RFC 2581, TCP Congestion Control, one of the most important TCP-related RFCs in recent years, describes updated algorithms that avoid undue congestion. In 2001, RFC 3168 was written to describe explicit congestion notification (ECN), a congestion avoidance signaling mechanism.

The original TCP congestion avoidance algorithm was known as "TCP Tahoe", but many alternative algorithms have since been proposed (including TCP Reno, TCP Vegas, FAST TCP, TCP New Reno, and TCP Hybla).

TCP Interactive (iTCP)<sup>[28]</sup> is a research effort into TCP extensions that allows applications to subscribe to TCP events and register handler components that can launch applications for various purposes, including application-assisted congestion control.

Multipath TCP (MPTCP)<sup>[29][30]</sup> is an ongoing effort within the IETF that aims at allowing a TCP connection to use multiple paths to maximise resource usage and increase redundancy. The redundancy offered by Multipath TCP in the context of wireless networks<sup>[31]</sup> enables statistical multiplexing of resources, and thus increases TCP throughput

dramatically. Multipath TCP also brings performance benefits in datacenter environments.<sup>[32]</sup> The reference implementation<sup>[33]</sup> of Multipath TCP is being developed in the Linux kernel.<sup>[34]</sup>

TCP Cookie Transactions (TCPCT) is an extension proposed in December 2009 to secure servers against denial-of-service attacks. Unlike SYN cookies, TCPCT does not conflict with other TCP extensions such as window scaling. TCPCT was designed due to necessities of DNSSEC, where servers have to handle large numbers of short-lived TCP connections.

tcpcrypt is an extension proposed in July 2010 to provide transport-level encryption directly in TCP itself. It is designed to work transparently and not require any configuration. Unlike TLS (SSL), tcpcrypt itself does not provide authentication, but provides simple primitives down to the application to do that. As of 2010, the first tcprypt IETF draft has been published and implementations exist for several major platforms.

TCP Fast Open is an extension to speed up the opening of successive TCP connections between two endpoints. It works by skipping the three-way handshake using a cryptographic "cookie". It is similar to an earlier proposal called T/TCP, which was not widely adopted due to security issues.<sup>[35]</sup> As of July 2012, it is an IETF Internet draft.<sup>[36]</sup>

## TCP over wireless networks

TCP has been optimized for wired networks. Any packet loss is considered to be the result of network congestion and the congestion window size is reduced dramatically as a precaution. However, wireless links are known to experience sporadic and usually temporary losses due to fading, shadowing, hand off, and other radio effects, that cannot be considered congestion. After the (erroneous) back-off of the congestion window size, due to wireless packet loss, there can be a congestion avoidance phase with a conservative decrease in window size. This causes the radio link to be underutilized. Extensive research has been done on the subject of how to combat these harmful effects. Suggested solutions can be categorized as end-to-end solutions (which require modifications at the client or server),<sup>[37]</sup> link layer solutions (such as RLP in cellular networks), or proxy based solutions (which require some changes in the network without modifying end nodes).<sup>[37][38]</sup>

A number of alternative congestion control algorithms have been proposed to help solve the wireless problem, such as Vegas, Westwood, Veno and Santa Cruz.

## Hardware implementations

One way to overcome the processing power requirements of TCP is to build hardware implementations of it, widely known as TCP Offload Engines (TOE). The main problem of TOEs is that they are hard to integrate into computing systems, requiring extensive changes in the operating system of the computer or device. One company to develop such a device was Alacritech.

## Debugging

A packet sniffer, which intercepts TCP traffic on a network link, can be useful in debugging networks, network stacks and applications that use TCP by showing the user what packets are passing through a link. Some networking stacks support the SO\_DEBUG socket option, which can be enabled on the socket using setsockopt. That option dumps all the packets, TCP states, and events on that socket, which is helpful in debugging. Netstat is another utility that can be used for debugging.

## Alternatives

For many applications TCP is not appropriate. One problem (at least with normal implementations) is that the application cannot access the packets coming after a lost packet until the retransmitted copy of the lost packet is received. This causes problems for real-time applications such as streaming media, real-time multiplayer games and voice over IP (VoIP) where it is generally more useful to get most of the data in a timely fashion than it is to get all of the data in order.

For both historical and performance reasons, most storage area networks (SANs) prefer to use Fibre Channel protocol (FCP) instead of TCP/IP.

Also, for embedded systems, network booting, and servers that serve simple requests from huge numbers of clients (e.g. DNS servers) the complexity of TCP can be a problem. Finally, some tricks such as transmitting data between two hosts that are both behind NAT (using STUN or similar systems) are far simpler without a relatively complex protocol like TCP in the way.

Generally, where TCP is unsuitable, the User Datagram Protocol (UDP) is used. This provides the application multiplexing and checksums that TCP does, but does not handle streams or retransmission, giving the application developer the ability to code them in a way suitable for the situation, or to replace them with other methods like forward error correction or interpolation.

SCTP is another IP protocol that provides reliable stream oriented services similar to TCP. It is newer and considerably more complex than TCP, and has not yet seen widespread deployment. However, it is especially designed to be used in situations where reliability and near-real-time considerations are important.

Venturi Transport Protocol (VTP) is a patented proprietary protocol that is designed to replace TCP transparently to overcome perceived inefficiencies related to wireless data transport.

TCP also has issues in high bandwidth environments. The TCP congestion avoidance algorithm works very well for ad-hoc environments where the data sender is not known in advance, but if the environment is predictable, a timing based protocol such as Asynchronous Transfer Mode (ATM) can avoid TCP's retransmits overhead.

Multipurpose Transaction Protocol (MTP/IP) is patented proprietary software that is designed to adaptively achieve high throughput and transaction performance in a wide variety of network conditions, particularly those where TCP is perceived to be inefficient.

## Checksum computation

### TCP checksum for IPv4

When TCP runs over IPv4, the method used to compute the checksum is defined in RFC 793:

*The checksum field is the 16 bit one's complement of the one's complement sum of all 16-bit words in the header and text. If a segment contains an odd number of header and text octets to be checksummed, the last octet is padded on the right with zeros to form a 16-bit word for checksum purposes. The pad is not transmitted as part of the segment. While computing the checksum, the checksum field itself is replaced with zeros.*

In other words, after appropriate padding, all 16-bit words are added using one's complement arithmetic. The sum is then bitwise complemented and inserted as the checksum field. A pseudo-header that mimics the IPv4 packet header used in the checksum computation is shown in the table below.

### TCP pseudo-header for checksum computation (IPv4)

Bit offset	0–3	4–7	8–15	16–31		
<b>0</b>	Source address					
<b>32</b>	Destination address					
<b>64</b>	Zeros		Protocol	TCP length		
<b>96</b>	Source port		Destination port			
<b>128</b>	Sequence number					
<b>160</b>	Acknowledgement number					
<b>192</b>	Data offset	Reserved	Flags	Window		
<b>224</b>	Checksum			Urgent pointer		
<b>256</b>	Options (optional)					
<b>256/288+</b>	Data					

The source and destination addresses are those of the IPv4 header. The protocol value is 6 for TCP (cf. List of IP protocol numbers). The TCP length field is the length of the TCP header and data.

### TCP checksum for IPv6

When TCP runs over IPv6, the method used to compute the checksum is changed, as per RFC 2460:

*Any transport or other upper-layer protocol that includes the addresses from the IP header in its checksum computation must be modified for use over IPv6, to include the 128-bit IPv6 addresses instead of 32-bit IPv4 addresses.*

A pseudo-header that mimics the IPv6 header for computation of the checksum is shown below.

### TCP pseudo-header for checksum computation (IPv6)

Bit offset	0–7	8–15	16–23	24–31		
<b>0</b>	Source address					
<b>32</b>						
<b>64</b>						
<b>96</b>						
<b>128</b>	Destination address					
<b>160</b>						
<b>192</b>						
<b>224</b>						
<b>256</b>	TCP length					
<b>288</b>	Zeros			Next header		
<b>320</b>	Source port		Destination port			
<b>352</b>	Sequence number					
<b>384</b>	Acknowledgement number					
<b>416</b>	Data offset	Reserved	Flags	Window		
<b>448</b>	Checksum			Urgent pointer		

<b>480</b>	Options (optional)
<b>480/512+</b>	Data

- Source address – the one in the IPv6 header
- Destination address – the final destination; if the IPv6 packet doesn't contain a Routing header, TCP uses the destination address in the IPv6 header, otherwise, at the originating node, it uses the address in the last element of the Routing header, and, at the receiving node, it uses the destination address in the IPv6 header.
- TCP length – the length of the TCP header and data
- Next Header – the protocol value for TCP

## Checksum offload

Many TCP/IP software stack implementations provide options to use hardware assistance to automatically compute the checksum in the network adapter prior to transmission onto the network or upon reception from the network for validation. This may relieve the OS from using precious CPU cycles calculating the checksum. Hence, overall network performance is increased.

This feature may cause packet analyzers detecting outbound network traffic upstream of the network adapter and unaware or uncertain about the use of checksum offload to report invalid checksum in outbound packets.

## References

- [1] Vinton G. Cerf, Robert E. Kahn, (May 1974). "A Protocol for Packet Network Intercommunication" (<http://ece.ut.ac.ir/Classpages/F84/PrincipleofNetworkDesign/Papers/CK74.pdf>). *IEEE Transactions on Communications* **22** (5): 637–648. .
- [2] Comer, Douglas E. (2006). *Internetworking with TCP/IP: Principles, Protocols, and Architecture*. **1** (5th ed.). Prentice Hall. ISBN 0-13-187671-6.
- [3] TCP (Linktionary term) (<http://www.linktionary.com/t/tcp.html>)
- [4] RFC 791 – section 2.1 (<http://tools.ietf.org/html/rfc791#section-2.1>)
- [5] RFC 793 (<http://tools.ietf.org/html/rfc793>)
- [6] RFC 793 section 3.1
- [7] RFC 1323, TCP Extensions for High Performance, Section 2.2 (<http://tools.ietf.org/html/rfc1323#page-9>)
- [8] RFC 2018, TCP Selective Acknowledgement Options, Section 2 (<http://tools.ietf.org/html/rfc2018#section-2>)
- [9] RFC 2018, TCP Selective Acknowledgement Options, Section 3 (<http://tools.ietf.org/html/rfc2018#section-3>)
- [10] RFC 1323, TCP Extensions for High Performance, Section 3.2 (<http://tools.ietf.org/html/rfc1323#page-11>)
- [11] RFC 1146, TCP Alternate Checksum Options (<http://tools.ietf.org/html/rfc1146#page-2>)
- [12] <http://www.medianet.kent.edu/techreports/TR2005-07-22-tcp-EFSM.pdf>
- [13] RFC 793 Section 3.2
- [14] Tanenbaum, Andrew S. (2003-03-17). *Computer Networks* (Fourth ed.). Prentice Hall. ISBN 0-13-066102-3.
- [15] <http://tools.ietf.org/html/rfc1122>
- [16] "TCP Definition" (<http://www.lin0.org/tcp.html>). . Retrieved 2011-03-12.
- [17] Stone; Partridge (2000). "When The CRC and TCP Checksum Disagree" (<http://citeseer.ist.psu.edu/stone00when.html>). *Sigcomm*.
- [18] RFC 879 (<http://www.faqs.org/rfcs/rfc879.html>)
- [19] TCP window scaling and broken routers [LWN.net] (<http://lwn.net/Articles/92727/>)
- [20] Gont, Fernando (2008-11). "On the implementation of TCP urgent data" (<http://www.gont.com.ar/talks/IETF73/ietf73-tcpm-urgent-data.ppt>). 73rd IETF meeting. . Retrieved 2009-01-04.
- [21] Peterson, Larry (2003). *Computer Networks*. Morgan Kaufmann. p. 401. ISBN 1-55860-832-X.
- [22] Richard W. Stevens (2006). *TCP/IP Illustrated. Vol. 1, The protocols* (<http://books.google.com/books?id=b2elQwAACAAJ>). Addison-Wesley. pp. Chapter 20. ISBN 978-0-201-63346-7.. Retrieved 14 November 2011.
- [23] Security Assessment of the Transmission Control Protocol (TCP) (<http://www.cpni.gov.uk/Docs/tn-03-09-security-assessment-TCP.pdf>)
- [24] Security Assessment of the Transmission Control Protocol (TCP) (<http://tools.ietf.org/html/draft-ietf-tcpm-tcp-security>)
- [25] Some insights about the recent TCP DoS (Denial of Service) vulnerabilities (<http://www.gont.com.ar/talks/hacklu2009/gont-hacklu2009-tcp-security.pdf>)
- [26] Exploiting TCP and the Persist Timer Infiniteness (<http://phrack.org/issues.html?issue=66&id=9#article>)
- [27] Laurent Joncheray, *Simple Active Attack Against TCP*, 1995 (<http://www.usenix.org/publications/library/proceedings/security95/joncheray.html>)

- [28] TCP Interactive (iTCP) ([http://www.medianet.kent.edu/projects\\_files/projectITCP.html](http://www.medianet.kent.edu/projects_files/projectITCP.html))
- [29] RFC 6182
- [30] <http://datatracker.ietf.org/doc/draft-ietf-mptcp-multiaddressed/> (<http://tools.ietf.org/html/draft-ietf-mptcp-multiaddressed>)
- [31] TCP with feed-forward source coding for wireless downlink networks (<http://portal.acm.org/citation.cfm?id=1794199>)
- [32] Raiciu; Barre; Pluntke; Greenhalgh; Wischik; Handley (2011). "Improving datacenter performance and robustness with multipath TCP" (<http://inl.info.ucl.ac.be/publications/improving-datacenter-performance-and-robustness-multipath-tcp>). *Sigcomm*.
- [33] MultiPath TCP - Linux Kernel implementation (<http://mptcp.info.ucl.ac.be/>)
- [34] Barre; Paasch; Bonaventure (2011). "MultiPath TCP: From Theory to Practice" (<http://inl.info.ucl.ac.be/publications/multipath-tcp-theory-practice>). *IFIP Networking*.
- [35] Michael Kerrisk (2012-08-01). "TCP Fast Open: expediting web services" (<https://lwn.net/SubscriberLink/508865/39212876277c174c/>). LWN.net. .
- [36] Y. Cheng, J. Chu, S. Radhakrishnan, A. Jain (2012-07-16). *TCP Fast Open* (<https://tools.ietf.org/html/draft-ictpm-fastopen-01>). IETF. I-D draft-ictpm-fastopen-01. .
- [37] "TCP performance over CDMA2000 RLP" (<http://academic.research.microsoft.com/Paper/3352358.aspx>). . Retrieved 2010-08-30
- [38] Muhammad Adeel & Ahmad Ali Iqbal (2004). "TCP Congestion Window Optimization for CDMA2000 Packet Data Networks" (<http://www.computer.org/portal/web/csdl/doi/10.1109/ITNG.2007.190>). *International Conference on Information Technology (ITNG'07)*: 31–35. doi:10.1109/ITNG.2007.190. ISBN 978-0-7695-2776-5. .

## Further reading

- W. Richard Stevens. TCP/IP Illustrated, Volume 1: The Protocols. ISBN 0-201-63346-9
- W. Richard Stevens and Gary R. Wright. TCP/IP Illustrated, Volume 2: The Implementation. ISBN 0-201-63354-X
- W. Richard Stevens. TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols. ISBN 0-201-63495-3

## External links

### RFC

- RFC 675 – Specification of Internet Transmission Control Program, December 1974 Version
- RFC 793 – TCP v4
- RFC 1122 – includes some error corrections for TCP
- RFC 1323 – TCP-Extensions
- RFC 1379 – Extending TCP for Transactions—Concepts
- RFC 1948 – Defending Against Sequence Number Attacks
- RFC 2018 – TCP Selective Acknowledgment Options
- RFC 4614 – A Roadmap for TCP Specification Documents
- RFC 5681 – TCP Congestion Control
- RFC 6298 – Computing TCP's Retransmission Timer

### Others

- Oral history interview with Robert E. Kahn (<http://purl.umn.edu/107387>), Charles Babbage Institute, University of Minnesota, Minneapolis. Focuses on Kahn's role in the development of computer networking from 1967 through the early 1980s. Beginning with his work at Bolt Beranek and Newman (BBN), Kahn discusses his involvement as the ARPANET proposal was being written, his decision to become active in its implementation, and his role in the public demonstration of the ARPANET. The interview continues into Kahn's involvement with networking when he moves to IPTO in 1972, where he was responsible for the administrative and technical evolution of the ARPANET, including programs in packet radio, the development of a new network protocol (TCP/IP), and the switch to TCP/IP to connect multiple networks.
- IANA Port Assignments (<http://www.iana.org/assignments/port-numbers>)

- John Kristoff's Overview of TCP (Fundamental concepts behind TCP and how it is used to transport data between two endpoints) (<http://condor.depaul.edu/~jkristof/technotes/tcp.html>)
- TCP fast retransmit simulation animated: slow start, sliding window, duplicated Ack, congestion window ([http://www.visualland.net/tcp\\_histroy.php?simu=tcp\\_fast\\_retransmit&protocol=TCP&title=4.Fast transmit&ctype=1](http://www.visualland.net/tcp_histroy.php?simu=tcp_fast_retransmit&protocol=TCP&title=4.Fast transmit&ctype=1))
- TCP, Transmission Control Protocol (<http://www.networksorcery.com/enp/protocol/tcp.htm>)
- Checksum example (<http://mathforum.org/library/drmath/view/54379.html>)
- Engineer Francesco Buffa's page about Transmission Control Protocol (<http://www.ilmondodeltelecomunicazioni.it/english/telematics/protocols.html>)
- TCP tutorial (<http://www.ssfnet.org/Exchange/tcp/tcpTutorialNotes.html>)
- Linktionary on TCP segments ([http://www.linktionary.com/s/segment\\_tcp.html](http://www.linktionary.com/s/segment_tcp.html))
- TCP Sliding Window simulation animated (ns2) ([http://www.visualland.net/tcp\\_histroy.php?simu=tcp\\_swnd&protocol=TCP&title=2.Sliding Window&ctype=1](http://www.visualland.net/tcp_histroy.php?simu=tcp_swnd&protocol=TCP&title=2.Sliding Window&ctype=1))
- Multipath TCP in Linux kernel (<http://inl.info.ucl.ac.be/mptcp>)

## Internet Protocol

---

The **Internet Protocol (IP)** is the principal communications protocol used for relaying datagrams (also known as network packets) across an internetwork using the Internet Protocol Suite. Responsible for routing packets across network boundaries, it is the primary protocol that establishes the Internet.

IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering datagrams from the source host to the destination host solely based on the addresses. For this purpose, IP defines datagram structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram source and destination.

Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974, the other being the connection-oriented Transmission Control Protocol (TCP). The Internet Protocol Suite is therefore often referred to as TCP/IP.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the internet. Its successor is Internet Protocol Version 6 (IPv6), which is increasing in use.

## Function

The Internet Protocol is responsible for addressing hosts and routing datagrams (packets) from a source host to the destination host across one or more IP networks. For this purpose the Internet Protocol defines an addressing system that has two functions: identifying hosts and providing a logical location service. This is accomplished by defining standard datagrams and a standard addressing system.

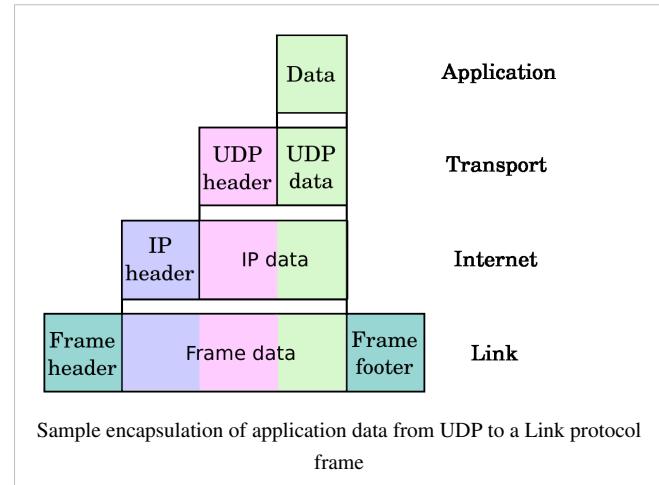
### Datagram construction

Each datagram has two components, a header and a payload. The IP header is tagged with the source IP address, destination IP address, and other meta-data needed to route and deliver the datagram. The payload is the data to be transported. This process of nesting data payloads in a packet with a header is called encapsulation.

### IP addressing and routing

Perhaps the most complex aspects of IP are IP addressing and routing. Addressing refers to how end hosts are assigned IP addresses and how subnetworks of IP host addresses are divided and grouped. IP routing is performed by all hosts, but most importantly by routers, which typically use either interior gateway protocols (IGPs) or external gateway protocols (EGPs) to decide how to move datagrams among networks.

IP routing is also common in local networks. For example, Ethernet switches sold today support IP multicast.<sup>[1]</sup> These switches use IP addresses and Internet Group Management Protocol for control of the multicast routing but use MAC addresses for the actual routing.



## Reliability

The design principles of the Internet protocols assume that the network infrastructure is inherently unreliable at any single network element or transmission medium and that it is dynamic in terms of availability of links and nodes. No central monitoring or performance measurement facility exists that tracks or maintains the state of the network. For the benefit of reducing network complexity, the intelligence in the network is purposely mostly located in the end nodes of each data transmission, cf. end-to-end principle. Routers in the transmission path simply forward packets to the next known local gateway matching the routing prefix for the destination address.

As a consequence of this design, the Internet Protocol only provides best effort delivery and its service is characterized as *unreliable*. In network architectural language it is a *connection-less* protocol, in contrast to so-called connection-oriented modes of transmission. The lack of reliability permits various error conditions, such as data corruption, packet loss and duplication, as well as out-of-order packet delivery. Since routing is dynamic for every packet and the network maintains no state of the path of prior packets, it is possible that some packets are routed on a longer path to their destination, resulting in improper sequencing at the receiver.

The only assistance that IPv4 provides regarding unreliability is to ensure that the IP packet header is error-free. A routing node calculates a checksum for a packet. If the checksum is bad, the routing node discards the packet. The routing node does not have to notify either end node, although the Internet Control Message Protocol (ICMP) allows such notification. In contrast, IPv6 abandons checksums in favor of faster routing.

Upper layer protocols are responsible for resolving reliability issues. For example, an upper layer protocol may cache data to make sure that it is in the correct order, before giving the data to an application.

In addition to issues of reliability, the dynamic nature and the diversity of the Internet and its components provide no guarantee that any particular path is actually capable of, or suitable for, performing the data transmission requested, even if the path is available and reliable. One of the technical constraints is the size of data packets allowed on a given link. An application must assure that it uses proper transmission characteristics. Some of this responsibility lies also in the upper layer protocols between application and IP. Facilities exist to examine the maximum transmission unit (MTU) size of the local link, as well as for the entire projected path to the destination when using IPv6. The IPv4 internetworking layer has the capability to automatically fragment the original datagram into smaller units for transmission. In this case, IP does provide re-ordering of fragments delivered out-of-order.<sup>[2]</sup>

Transmission Control Protocol (TCP) is an example of a protocol that will adjust its segment size to be smaller than the MTU. User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP) disregard MTU size, thereby forcing IP to fragment oversized datagrams.<sup>[3]</sup>

## Version history

In May 1974, the Institute of Electrical and Electronic Engineers (IEEE) published a paper entitled "A Protocol for Packet Network Intercommunication."<sup>[4]</sup> The paper's authors, Vint Cerf and Bob Kahn, described an internetworking protocol for sharing resources using packet-switching among the nodes. A central control component of this model was the "Transmission Control Program" (TCP) that incorporated both connection-oriented links and datagram services between hosts. The monolithic Transmission Control Program was later divided into a modular architecture consisting of the Transmission Control Protocol at the connection-oriented layer and the Internet Protocol at the internetworking (datagram) layer. The model became known informally as TCP/IP, although formally referenced as the Internet Protocol Suite.

The Internet Protocol is one of the elements that define the Internet. The dominant internetworking protocol in the Internet Layer in use today is IPv4; the number 4 is the protocol version number carried in every IP datagram. IPv4 is described in RFC 791 (1981).

The successor to IPv4 is IPv6. Its most prominent modification from version 4 is the addressing system. IPv4 uses 32-bit addresses (c. 4 billion, or  $4.3 \times 10^9$ , addresses) while IPv6 uses 128-bit addresses (c. 340 undecillion, or  $3.4 \times 10^{38}$  addresses). Although adoption of IPv6 has been slow, as of June 2008, all United States government systems have demonstrated basic infrastructure support for IPv6 (if only at the backbone level).<sup>[5]</sup>

IP versions 0 to 3 were development versions of IPv4 and were used between 1977 and 1979. Version 5 was used by the Internet Stream Protocol, an experimental streaming protocol. Version numbers 6 through 9 were proposed for various protocol models designed to replace IPv4: SIPP (Simple Internet Protocol Plus, known now as IPv6), TP/IX (RFC 1475), PIP (RFC 1621) and TUBA (TCP and UDP with Bigger Addresses, RFC 1347).

Other protocol proposals named *IPv9* and *IPv8* briefly surfaced, but have no support.<sup>[6]</sup>

On April 1, 1994, the IETF published an April Fool's Day joke about IPv9.<sup>[7]</sup>

## Vulnerabilities

The Internet Protocol is vulnerable to a variety of attacks. A thorough vulnerability assessment, along with proposed mitigations, was published in 2008,<sup>[8]</sup> and is currently being pursued within the IETF.<sup>[9]</sup>

## References

- [1] Netgear ProSafe XSM7224S reference manual
- [2] Siyan, Karanjit. *Inside TCP/IP*, New Riders Publishing, 1997. ISBN 1-56205-714-6
- [3] Basic Journey of a Packet (<http://www.securityfocus.com/infocus/1870>)
- [4] Vinton G. Cerf, Robert E. Kahn, "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Vol. 22, No. 5, May 1974 pp. 637-648
- [5] CIO council adds to IPv6 transition primer ([http://www.gcn.com/print/25\\_16/41051-1.html](http://www.gcn.com/print/25_16/41051-1.html)), gcn.com
- [6] Theregister.com ([http://www.theregister.co.uk/2004/07/06/ipv9\\_hype\\_dismissed/](http://www.theregister.co.uk/2004/07/06/ipv9_hype_dismissed/))
- [7] RFC 1606: *A Historical Perspective On The Usage Of IP Version 9*. April 1, 1994.
- [8] Security Assessment of the Internet Protocol (IP)(archived version) (<http://web.archive.org/web/20100211145721/http://www.cpan.gov.uk/Docs/InternetProtocol.pdf>)
- [9] Security Assessment of the Internet Protocol version 4 (IPv4) (<http://tools.ietf.org/html/draft-ietf-opsec-ip-security>)

## External links

- Internet Protocol (<http://www.dmoz.org/Computers/Internet/Protocols/>) at the Open Directory Project
- RFC 791
- Data Communication Lectures of Manfred Lindner - Part IP Technology Basics ([http://www.ict.tuwien.ac.at/lva/384.081/infobase/L30-IP\\_Technology\\_Basics\\_v4-6.pdf](http://www.ict.tuwien.ac.at/lva/384.081/infobase/L30-IP_Technology_Basics_v4-6.pdf))
- Data Communication Lectures of Manfred Lindner - Part IP Technology Details ([http://www.ict.tuwien.ac.at/lva/384.081/infobase/L31-IP\\_Technology\\_Details\\_v4-7.pdf](http://www.ict.tuwien.ac.at/lva/384.081/infobase/L31-IP_Technology_Details_v4-7.pdf))
- Data Communication Lectures of Manfred Lindner - Part IPv6 ([http://www.ict.tuwien.ac.at/lva/384.081/infobase/L80-IPv6\\_v4-6.pdf](http://www.ict.tuwien.ac.at/lva/384.081/infobase/L80-IPv6_v4-6.pdf))
- IPv6.com - Knowledge Center for Next Generation Internet IPv6 (<http://www.ipv6.com>)

# IPv4

**Internet Protocol version 4 (IPv4)** is the fourth revision in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet. As of 2012 IPv4 is still the most widely deployed Internet Layer protocol.

IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).

IPv4 is a connectionless protocol for use on packet-switched Link Layer networks (e.g., Ethernet). It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).

## Addressing

IPv4 uses 32-bit (four-byte) addresses, which limits the address space to  $4294967296 (2^{32})$  addresses. Addresses were assigned to users, and the number of unassigned addresses decreased. IPv4 address exhaustion occurred on February 3, 2011. It had been significantly delayed by address changes such as classful network design, Classless Inter-Domain Routing, and network address translation (NAT).

This limitation of IPv4 stimulated the development of IPv6 in the 1990s, which has been in commercial deployment since 2006.

IPv4 reserves special address blocks for private networks (~18 million addresses) and multicast addresses (~270 million addresses).

## Address representations

IPv4 addresses may be written in any notation expressing a 32-bit integer value, but for human convenience, they are most often written in the dot-decimal notation, which consists of four octets of the address expressed individually in decimal and separated by periods.

The following table shows several representation formats:

Notation	Value	Conversion from dot-decimal
Dotted decimal	192.0.2.235	N/A
Dotted hexadecimal <sup>[1]</sup>	0xC0.0x00.0x02.0xEB	Each octet is individually converted to hexadecimal form
Dotted octal <sup>[1]</sup>	0300.0000.0002.0353	Each octet is individually converted into octal
Hexadecimal	0xC00002EB	Concatenation of the octets from the dotted hexadecimal
Decimal	3221226219	The 32-bit number expressed in decimal
Octal	030000001353	The 32-bit number expressed in octal

## Allocation

Originally, an IP address was divided into two parts: the network identifier was the most significant (highest order) octet of the address, and the host identifier was the rest of the address. The latter was therefore also called the *rest field*. This enabled the creation of a maximum of 256 networks. This was quickly found to be inadequate.

To overcome this limit, the high order octet of the addresses was redefined to create a set of *classes* of networks, in a system which later became known as classful networking. The system defined five classes, Class A, B, C, D, and E. The Classes A, B, and C had different bit lengths for the new network identification. The rest of an address was used as previously to identify a host within a network, which meant that each network class had a different capacity to address hosts. Class D was allocated for multicast addressing and Class E was reserved for future applications.

Starting around 1985, people devised methods to subdivide IP networks. One flexible method was the *variable-length subnet mask* (VLSM).<sup>[2][3]</sup>

Around 1993, this system of classes was officially replaced with Classless Inter-Domain Routing (CIDR), and the class-based scheme was dubbed *classful*, by contrast. CIDR was designed to permit repartitioning of any address space so that smaller or larger blocks of addresses could be allocated to users. The hierarchical structure created by CIDR is managed by the Internet Assigned Numbers Authority (IANA) and the regional Internet registries (RIRs). Each RIR maintains a publicly searchable WHOIS database that provides information about IP address assignments.

## Special-use addresses

### Reserved address blocks

Range	Description	Reference
0.0.0.0/8	Current network (only valid as source address)	RFC 1700
10.0.0.0/8	Private network	RFC 1918
100.64.0.0/10	Shared Address Space	RFC 6598
127.0.0.0/8	Loopback	RFC 5735
169.254.0.0/16	Link-local	RFC 3927
172.16.0.0/12	Private network	RFC 1918
192.0.0.0/24	Reserved (IANA)	RFC 5735
192.0.2.0/24	TEST-NET-1, documentation and examples	RFC 5735
192.88.99.0/24	IPv6 to IPv4 relay	RFC 3068
192.168.0.0/16	Private network	RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
198.51.100.0/24	TEST-NET-2, documentation and examples	RFC 5737
203.0.113.0/24	TEST-NET-3, documentation and examples	RFC 5737
224.0.0.0/4	IP multicast (former Class D network)	RFC 5771
240.0.0.0/4	Reserved (former Class E network)	RFC 1700
255.255.255.255	Broadcast	RFC 919

## Private networks

Of the approximately four billion addresses allowed in IPv4, three ranges of address are reserved for use in private networks. These ranges are not routable outside of private networks, and private machines cannot directly communicate with public networks. They can, however, do so through network address translation.

The following are the three ranges reserved for private networks (RFC 1918):

Name	Address range	Number of addresses	Classful description	Largest CIDR block
24-bit block	10.0.0.0–10.255.255.255	16777216	Single Class A	10.0.0.0/8
20-bit block	172.16.0.0–172.31.255.255	1048576	Contiguous range of 16 Class B blocks	172.16.0.0/12
16-bit block	192.168.0.0–192.168.255.255	65536	Contiguous range of 256 Class C blocks	192.168.0.0/16

## Virtual private networks

Packets with a private destination address are ignored by all public routers. Two private networks (e.g., two branch offices) cannot communicate via the public internet, unless they use an IP tunnel or a virtual private network (VPN). When one private network wants to send a packet to another private network, the first private network encapsulates the packet in a protocol layer so that the packet can travel through the public network. Then the packet travels through the public network. When the packet reaches the other private network, its protocol layer is removed, and the packet travels to its destination.

Optionally, encapsulated packets may be encrypted to secure the data while it travels over the public network.

## Link-local addressing

RFC 5735 defines the special address block 169.254.0.0/16 for link-local addressing. These addresses are only valid on links (such as a local network segment or point-to-point connection) connected to a host. These addresses are not routable. Like private addresses, these addresses cannot be the source or destination of packets traversing the internet. These addresses are primarily used for address autoconfiguration (Zeroconf) when a host cannot obtain an IP address from a DHCP server or other internal configuration methods.

When the address block was reserved, no standards existed for address autoconfiguration. Microsoft created an implementation called Automatic Private IP Addressing (APIPA), which was deployed on millions of machines and became a de facto standard. Many years later, in May 2005, the IETF defined a formal standard in RFC 3927, entitled *Dynamic Configuration of IPv4 Link-Local Addresses*.

## Loopback

The class A network 127.0.0.0 (classless network 127.0.0.0/8) is reserved for loopback. IP packets which source addresses belong to this network should never appear outside a host. The modus operandi of this network expands upon that of a loopback interface:

- IP packets which source and destination addresses belong to the network (or subnetwork) of the same loopback interface are returned back to that interface;
- IP packets which source and destination addresses belong to networks (or subnetworks) of different interfaces of the same host, one of them being a loopback interface, are forwarded regularly.

## Addresses ending in 0 or 255

Networks with subnet masks of at least 24 bits, i.e. Class C networks in classful networking, and networks with CIDR prefixes /24 to /32 (255.255.255.0–255.255.255.255) may not have an address ending in 0 or 255.

Classful addressing prescribed only three possible subnet masks: Class A, 255.0.0.0 or /8; Class B, 255.255.0.0 or /16; and Class C, 255.255.255.0 or /24. For example, in the subnet 192.168.5.0/255.255.255.0 (192.168.5.0/24) the identifier 192.168.5.0 commonly is used to refer to the entire subnet. To avoid ambiguity in representation, the address ending in the octet 0 is reserved.

A broadcast address is an address that allows information to be sent to all interfaces in a given subnet, rather than a specific machine. Generally, the broadcast address is found by obtaining the bit complement of the subnet mask and performing a bitwise OR operation with the network identifier. In other words, the broadcast address is the last address in the address range of the subnet. For example, the broadcast address for the network 192.168.5.0 is 192.168.5.255. For networks of size /24 or larger, the broadcast address always ends in 255.

However, this does not mean that every address ending in 0 or 255 cannot be used as a host address. For example, consider a /16 subnet 192.168.0.0/255.255.0.0, which is equivalent to the address range 192.168.0.0–192.168.255.255. The broadcast address is 192.168.255.255. One can use the following addresses for hosts, even though they end with 255: 192.168.1.255, 192.168.2.255, etc. Also, 192.168.0.0 is the network identifier and must not be used for a host.<sup>[4]</sup> One can use the following addresses for hosts, even though they end with 0: 192.168.1.0, 192.168.2.0, etc.

In the past, conflict between network addresses and broadcast addresses arose because some software used non-standard broadcast addresses with zeros instead of ones.<sup>[5]</sup>

In networks smaller than /24, broadcast addresses do not necessarily end with 255. For example, a CIDR subnet 203.0.113.16/28 has the broadcast address 203.0.113.31.

## Address resolution

Hosts on the Internet are usually known by names, e.g., www.example.com, not primarily by their IP address, which is used for routing and network interface identification. The use of domain names requires translating, called *resolving*, them to addresses and vice versa. This is analogous to looking up a phone number in a phone book using the recipient's name.

The translation between addresses and domain names is performed by the Domain Name System (DNS), a hierarchical, distributed naming system which allows for subdelegation of name spaces to other DNS servers. DNS is often described in analogy to the telephone system directory information systems in which subscriber names are translated to telephone numbers.

## Address space exhaustion

Since the 1980s, it was apparent that the pool of available IPv4 addresses was being depleted at a rate that was not initially anticipated in the original design of the network address system.<sup>[6]</sup> The threat of exhaustion was the motivation for remedial technologies, such as classful networks, Classless Inter-Domain Routing (CIDR) methods, and network address translation (NAT). Eventually, IPv6 was created, which has many more addresses available.

Several market forces accelerated IPv4 address exhaustion:

- Rapidly growing number of Internet users
- Always-on devices — ADSL modems, cable modems
- Mobile devices — laptop computers, PDAs, mobile phones

Some technologies mitigated IPv4 address exhaustion:

- Network address translation (NAT) is a technology that allows a private network to use one public IP address. It permits private addresses in the private network.
- Use of private networks
- Dynamic Host Configuration Protocol (DHCP)
- Name-based virtual hosting of web sites
- Tighter control by regional Internet registries over the allocation of addresses to local Internet registries
- Network renumbering to reclaim large blocks of address space allocated in the early days of the Internet

The primary address pool of the Internet, maintained by IANA, was exhausted on 3 February 2011, when the last 5 blocks were allocated to the 5 RIRs.<sup>[7][8]</sup> APNIC was the first RIR to exhaust its regional pool on 15 April 2011, except for a small amount of address space reserved for the transition to IPv6, which will be allocated under a much more restricted policy.<sup>[9]</sup>

The accepted and standard solution is to use Internet Protocol Version 6. The address size was increased in IPv6 to 128 bits, providing a vastly increased address space that also allows improved route aggregation across the Internet and offers large subnetwork allocations of a minimum of  $2^{64}$  host addresses to end-users. Migration to IPv6 is in progress but completion is expected to take considerable time.

## Packet structure

An IP packet consists of a header section and a data section.

### Header

The IPv4 packet header consists of 14 fields, of which 13 are required. The 14th field is optional (red background in table) and aptly named: options. The fields in the header are packed with the most significant byte first (big endian), and for the diagram and discussion, the most significant bits are considered to come first (MSB 0 bit numbering). The most significant bit is numbered 0, so the version field is actually found in the four most significant bits of the first byte, for example.

**IPv4 Header Format**

Offsets	Octet	0				1				2				3																							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
0	0	<i>Version</i>		<i>IHL</i>		<i>DSCP</i>				<i>ECN</i>				<i>Total Length</i>																							
4	32	<i>Identification</i>										<i>Flags</i>		<i>Fragment Offset</i>																							
8	64	<i>Time To Live</i>				<i>Protocol</i>				<i>Header Checksum</i>																											
12	96	<i>Source IP Address</i>																																			
16	128	<i>Destination IP Address</i>																																			
20	160	<i>Options (if IHL &gt; 5)</i>																																			

#### Version

The first header field in an IP packet is the four-bit version field. For IPv4, this has a value of 4 (hence the name IPv4).

#### Internet Header Length (IHL)

The second field (4 bits) is the Internet Header Length (IHL), which is the number of 32-bit words in the header. Since an IPv4 header may contain a variable number of options, this field specifies the size of the header (this also coincides with the offset to the data). The minimum value for this field is 5 (RFC 791), which is a length of  $5 \times 32 = 160$  bits = 20 bytes. Being a 4-bit value, the maximum length is 15 words ( $15 \times 32$  bits) or

480 bits = 60 bytes.

#### Differentiated Services Code Point (DSCP)

Originally defined as the Type of Service field, this field is now defined by RFC 2474 for Differentiated services (DiffServ). New technologies are emerging that require real-time data streaming and therefore make use of the DSCP field. An example is Voice over IP (VoIP), which is used for interactive data voice exchange.

#### Explicit Congestion Notification (ECN)

This field is defined in RFC 3168 and allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature that is only used when both endpoints support it and are willing to use it. It is only effective when supported by the underlying network.

#### Total Length

This 16-bit field defines the entire packet (fragment) size, including header and data, in bytes. The minimum-length packet is 20 bytes (20-byte header + 0 bytes data) and the maximum is 65,535 bytes — the maximum value of a 16-bit word. The largest datagram that any host is required to be able to reassemble is 576 bytes, but most modern hosts handle much larger packets. Sometimes subnetworks impose further restrictions on the packet size, in which case datagrams must be fragmented. Fragmentation is handled in either the host or router in IPv4.

#### Identification

This field is an identification field and is primarily used for uniquely identifying fragments of an original IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to help trace datagrams with spoofed source addresses.<sup>[10]</sup>

#### Flags

A three-bit field follows and is used to control or identify fragments. They are (in order, from high order to low order):

- bit 0: Reserved; must be zero.<sup>[11]</sup>
- bit 1: Don't Fragment (DF)
- bit 2: More Fragments (MF)

If the DF flag is set, and fragmentation is required to route the packet, then the packet is dropped. This can be used when sending packets to a host that does not have sufficient resources to handle fragmentation. It can also be used for Path MTU Discovery, either automatically by the host IP software, or manually using diagnostic tools such as ping or traceroute.

For unfragmented packets, the MF flag is cleared. For fragmented packets, all fragments except the last have the MF flag set. The last fragment has a non-zero Fragment Offset field, differentiating it from an unfragmented packet.

#### Fragment Offset

The fragment offset field, measured in units of eight-byte blocks, is 13 bits long and specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram. The first fragment has an offset of zero. This allows a maximum offset of  $(2^{13} - 1) \times 8 = 65,528$  bytes, which would exceed the maximum IP packet length of 65,535 bytes with the header length included ( $65,528 + 20 = 65,548$  bytes).

#### Time To Live (TTL)

An eight-bit time to live field helps prevent datagrams from persisting (e.g. going in circles) on an internet. This field limits a datagram's lifetime. It is specified in seconds, but time intervals less than 1 second are rounded up to 1. In practice, the field has become a hop count—when the datagram arrives at a router, the router decrements the TTL field by one. When the TTL field hits zero, the router discards the packet and typically sends a ICMP Time Exceeded message to the sender.

The program traceroute uses these ICMP Time Exceeded messages to print the routers used by packets to go from the source to the destination.

#### Protocol

This field defines the protocol used in the data portion of the IP datagram. The Internet Assigned Numbers Authority maintains a list of IP protocol numbers which was originally defined in RFC 790.

#### Header Checksum

The 16-bit checksum field is used for error-checking of the header. When a packet arrives at a router, the router calculates the checksum of the header and compares it to the checksum field. If the values do not match, the router discards the packet. Errors in the data field must be handled by the encapsulated protocol. Both UDP and TCP have checksum fields.

When a packet arrives at a router, the router decreases the TTL field. Consequently, the router must calculate a new checksum. RFC 1071 defines the checksum calculation:

*The checksum field is the 16-bit one's complement of the one's complement sum of all 16-bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero.*

For example, consider Hex 4500003044224000800600008c7c19acae241e2b (20 bytes IP header):

Step 1)  $4500 + 0030 + 4422 + 4000 + 8006 + 0000 + 8c7c + 19ac + ae24 + 1e2b = 2BBCF$  (16-bit sum)

Step 2)  $2 + BBCF = BBD1 = 1011101111010001$  (1's complement 16-bit sum)

Step 3)  $\sim BBD1 = 0100010000101110 = 442E$  (1's complement of 1's complement 16-bit sum)

To validate a header's checksum the same algorithm may be used - the checksum of a header which contains a correct checksum field is a word containing all zeros (value 0):

$2BBCF + 442E = 2FFFD$ .  $2 + FFFD = FFFF$ . the 1'S of  $FFFF = 0$ .

#### Source address

This field is the IPv4 address of the sender of the packet. Note that this address may be changed in transit by a network address translation device.

#### Destination address

This field is the IPv4 address of the receiver of the packet. As with the source address, this may be changed in transit by a network address translation device.

#### Options

The options field is not often used. Note that the value in the IHL field must include enough extra 32-bit words to hold all the options (plus any padding needed to ensure that the header contains an integral number of 32-bit words). The list of options may be terminated with an EOL (End of Options List, 0x00) option; this is only necessary if the end of the options would not otherwise coincide with the end of the header. The possible options that can be put in the header are as follows:

Field	Size (bits)	Description
Copied	1	Set to 1 if the options need to be copied into all fragments of a fragmented packet.
Option Class	2	A general options category. 0 is for "control" options, and 2 is for "debugging and measurement". 1, and 3 are reserved.
Option Number	5	Specifies an option.
Option Length	8	Indicates the size of the entire option (including this field). This field may not exist for simple options.
Option Data	Variable	Option-specific data. This field may not exist for simple options.

- Note: If the header length is greater than 5, i.e. it is from 6 to 15, it means that the options field is present and must be considered.
- Note: Copied, Option Class, and Option Number are sometimes referred to as a single eight-bit field - the *Option Type*.

The following two options are discouraged because they create security concerns: Loose Source and Record Route (LSRR) and Strict Source and Record Route (SSRR). Many routers block packets containing these options.<sup>[12]</sup>

## Data

The data portion of the packet is not included in the packet checksum. Its contents are interpreted based on the value of the Protocol header field.

In a typical IP implementation, standard protocols such as TCP and UDP are implemented in the OS kernel, for performance reasons. Other protocols such as ICMP may be partially implemented by the kernel, or implemented purely in user software. Protocols not implemented in-kernel, and not exposed by standard APIs such as BSD sockets, are typically implemented using a 'raw socket' API.

Some of the common protocols for the data portion are listed below:

Protocol Number	Protocol Name	Abbreviation
1	Internet Control Message Protocol	ICMP
2	Internet Group Management Protocol	IGMP
6	Transmission Control Protocol	TCP
17	User Datagram Protocol	UDP
41	IPv6 encapsulation	ENCAP
89	Open Shortest Path First	OSPF
132	Stream Control Transmission Protocol	SCTP

See List of IP protocol numbers for a complete list.

## Fragmentation and reassembly

The Internet Protocol enables networks to communicate with one another. The design accommodates networks of diverse physical nature; it is independent of the underlying transmission technology used in the Link Layer. Networks with different hardware usually vary not only in transmission speed, but also in the maximum transmission unit (MTU). When one network wants to transmit datagrams to a network with a smaller MTU, it may fragment its datagrams. In IPv4, this function was placed at the Internet Layer, and is performed in IPv4 routers, which thus only

require this layer as the highest one implemented in their design.

In contrast, IPv6, the next generation of the Internet Protocol, does not require routers to perform fragmentation; hosts must determine the path MTU before sending datagrams.

## Fragmentation

When a router receives a packet, it examines the destination address and determines the outgoing interface to use. The interface has an MTU. If the packet size is bigger than the MTU, the router may fragment the packet.

The router divides the packet into segments. The max size of each segment is the MTU minus the IP header size (20 bytes minimum; 60 bytes maximum). The router puts each segment into its own packet, each fragment packet having following changes:

- The *total length* field is the segment size.
- The *more fragments* (MF) flag is set for all segments except the last one, which is set to 0.
- The *fragment offset* field is set, based on the offset of the segment in the original data payload. This is measured in units of eight-byte blocks.
- The *header checksum* field is recomputed.

For example, for an MTU of 1,500 bytes and a header size of 20 bytes, the fragment offsets would be multiples of  $(1500 - 20)/8 = 185$ . These multiples are 0, 185, 370, 555, 740, ...

It is possible for a packet to be fragmented at one router, and for the fragments to be fragmented at another router. For example, consider a packet with a data size of 4,500 bytes, no options, and a header size of 20 bytes. So the packet size is 4,520 bytes. Assume that the packet travels over a link with an MTU of 2,500 bytes. Then it will become two fragments:

Fragment	Total bytes	Header bytes	Data bytes	"More fragments" flag	Fragment offset (bytes)
1	2500	20	2480	1	0
2	2040	20	2020	0	310

Note that the fragments preserve the data size:  $2480 + 2020 = 4500$ .

Note how we get the offsets from the data sizes:

- 0.
- $0 + 2480/8 = 310$ .

Assume that these fragments reach a link with an MTU of 1,500 bytes. Each fragment will become two fragments:

Fragment	Total bytes	Header bytes	Data bytes	"More fragments" flag	Fragment offset (bytes)
1	1500	20	1480	1	0
2	1020	20	1000	1	185
3	1500	20	1480	1	310
4	560	20	540	0	495

Note that the fragments preserve the data size:  $1480 + 1000 = 2480$ , and  $1480 + 540 = 2020$ .

Note how we get the offsets from the data sizes:

- 0.
- $0 + 1480/8 = 185$
- $185 + 1000/8 = 310$
- $310 + 1480/8 = 495$

We can use the last offset and last data size to calculate the total data size:  $495*8 + 540 = 3960 + 540 = 4500$ .

## Reassembly

A receiver knows that a packet is a fragment if at least one of the following conditions is true:

- The "more fragments" flag is set. (This is true for all fragments except the last.)
- The "fragment offset" field is nonzero. (This is true for all fragments except the first.)

The receiver identifies matching fragments using the identification field. The receiver will reassemble the data from fragments with the same identification field using both the fragment offset and the more fragments flag. When the receiver receives the last fragment (which has the "more fragments" flag set to 0), it can calculate the length of the original data payload, by multiplying the last fragment's offset by eight, and adding the last fragment's data size. In the example above, this calculation was  $495*8 + 540 = 4500$  bytes.

When the receiver has all the fragments, it can put them in the correct order, by using their offsets. It can then pass their data up the stack for further processing.

## Assistive protocols

The Internet Protocol is the protocol that defines and enables internetworking at the Internet Layer and thus forms the Internet. It uses a logical addressing system. IP addresses are not tied in any permanent manner to hardware identifications and, indeed, a network interface can have multiple IP addresses. Hosts and routers need additional mechanisms to identify the relationship between device interfaces and IP addresses, in order to properly deliver an IP packet to the destination host on a link. The Address Resolution Protocol (ARP) performs this IP-address-to-hardware-address translation for IPv4. (A hardware address is also called a MAC address.) In addition, the reverse correlation is often necessary. For example, when an IP host is booted or connected to a network it needs to determine its IP address, unless an address is preconfigured by an administrator. Protocols for such inverse correlations exist in the Internet Protocol Suite. Currently used methods are Dynamic Host Configuration Protocol (DHCP), Bootstrap Protocol (BOOTP) and, infrequently, reverse ARP.

## Notes

- [1] "INET(3) man page" ([http://www.unix.com/man-page/Linux/3/inet\\_addr/](http://www.unix.com/man-page/Linux/3/inet_addr/)). . Retrieved 2010-11-28.
- [2] "Planning Classless Routing: TCP/IP" ([http://technet.microsoft.com/en-us/library/cc779089\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc779089(WS.10).aspx)). Technet.microsoft.com. 2003-03-28. . Retrieved 2012-01-20.
- [3] "HP Networking: switches, routers, wired, wireless, HP TippingPoint Security" ([http://www.3com.com/other/pdfs/infra/corpinfo/en\\_US/501302.pdf](http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf)). 3com.com. . Retrieved 2012-01-20.
- [4] Robert Braden (October 1989). "Requirements for Internet Hosts -- Communication Layers" (<http://tools.ietf.org/html/rfc1122#page-31>). IETF. p. 31. RFC 1122. .
- [5] Robert Braden (October 1989). "Requirements for Internet Hosts -- Communication Layers" (<http://tools.ietf.org/html/rfc1122#page-66>). IETF. p. 66. RFC 1122. .
- [6] "World 'running out of Internet addresses'" (<http://technology.inquirer.net/infotech/infotech/view/20110121-315808/World-running-out-of-Internet-addresses>). . Retrieved 2011-01-23.
- [7] Smith, Lucie; Lipner, Ian (3 February 2011). "Free Pool of IPv4 Address Space Depleted" (<http://www.nro.net/news/ipv4-free-pool-depleted>). Number Resource Organization. . Retrieved 3 February 2011.
- [8] ICANN,nanog mailing list. "Five /8s allocated to RIRs - no unallocated IPv4 unicast /8s remain" (<http://mailman.nanog.org/pipermail/nanog/2011-February/032107.html>). .
- [9] Asia-Pacific Network Information Centre (15 April 2011). "APNIC IPv4 Address Pool Reaches Final /8" (<http://www.apnic.net/publications/news/2011/final-8>). . Retrieved 15 April 2011.
- [10] Savage, Stefan. "Practical network support for IP traceback" (<http://portal.acm.org/citation.cfm?id=347057.347560>). . Retrieved 2010-09-06.
- [11] As an April Fools' joke, proposed for use in RFC 3514 as the "Evil bit".
- [12] "Cisco unofficial FAQ" (<http://www.faqs.org/faqs/cisco-networking-faq/section-23.html>). . Retrieved 2012-05-10.

## References

### External links

- RFC 791 — Internet Protocol
- <http://www.iana.org> — Internet Assigned Numbers Authority (IANA)
- <http://www.networksorcery.com/enp/protocol/ip.htm> — IP Header Breakdown, including specific options
- RFC 3344 — IPv4 Mobility
- IPv6 vs. carrier-grade NAT/squeezing more out of IPv4 (<http://www.networkworld.com/news/2010/060710-tech-argument-ipv6-nat.html>)

Address exhaustion:

- RIPE report on address consumption as of October 2003 (<http://www.ripe.net/rs/news/ipv4-ncc-20031030.html>)
- Official current state of IPv4 /8 allocations, as maintained by IANA (<http://www.iana.org/assignments/ipv4-address-space>)
- Dynamically generated graphs of IPv4 address consumption with predictions of exhaustion dates — Geoff Huston (<http://www.potaroo.net/tools/ipv4/index.html>)
- IP addressing in China and the myth of address shortage (<http://www.apnic.net/community/about-the-internet-community/internet-governance/articles/ip-addressing-in-china-2004>)
- Countdown of remaining IPv4 available addresses ([http://www.inetcore.com/project/ipv4ec/index\\_en.html](http://www.inetcore.com/project/ipv4ec/index_en.html)) (estimated)

## IPv4 address exhaustion

**IPv4 address exhaustion** is the depletion of the pool of unallocated Internet Protocol Version 4 (IPv4) addresses. The IP address space is managed by the Internet Assigned Numbers Authority (IANA) globally, and by five regional Internet registries (RIR) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers. With IANA's exhaustion on 31 January 2011,<sup>[1][2][3]</sup> and the RIR APNIC's exhaustion on 15 April 2011, some parts of the world have already exhausted their IPv4 allocations,<sup>[4][5][6]</sup> and the remaining RIRs are expected to deplete their pools within a few years.<sup>[5]</sup>

IPv4 provides approximately 4.29 billion addresses; a subset of these have been distributed by IANA to the RIRs in blocks of approximately 16.8 million addresses each. The depletion of the IPv4 allocation pool has been a concern since the late 1980s, when the Internet started to experience dramatic growth. The Internet Engineering Task Force (IETF) created the Routing and Addressing Group (ROAD) in November 1991 to respond to the scalability problem caused by the classful network allocation system in place at the time.<sup>[7][8]</sup> The anticipated shortage has been the driving factor in creating and adopting several new technologies, including Classless Inter-Domain Routing (CIDR) in 1993, network address translation (NAT), and IPv6 in 1998;<sup>[8]</sup> IPv6 (Internet Protocol Version 6), which can support about  $3.4 \times 10^{38}$  addresses, is the IETF's successor technology to IPv4.<sup>[9]</sup>

Although the predicted depletion was already approaching its final stages in 2008, most providers of Internet services and software vendors were just beginning IPv6 deployment.<sup>[10]</sup>

## IP addressing

Every node of an Internet Protocol (IP) network, such as a computer, router, or network printer, is assigned an IP address that is used to locate and identify the node in communications with other nodes on the network. Internet Protocol version 4 provides  $2^{32}$  (4,294,967,296) addresses. However, large blocks of IPv4 addresses are reserved for special uses and are unavailable for public allocation.

The IPv4 addressing structure provides an insufficient number of publicly routable addresses to provide a distinct address to every Internet device or service. This problem has been mitigated for some time by changes in the address allocation and routing infrastructure of the Internet. The transition from classful network addressing to Classless Inter-Domain Routing delayed the exhaustion of addresses substantially.

In addition, network address translation (NAT) permits Internet service providers and enterprises to masquerade private network address space with only one publicly routable IPv4 address on the Internet interface of a customer premise router, instead of allocating a public address to each network device. Complicating matters, IPv6 unaware NATs break native and 6to4 IPv6 connectivity, and a large fraction break 6in4 tunnels.

## Address depletion

While the primary reason for IPv4 address exhaustion is insufficient design capacity of the original Internet infrastructure, several additional driving factors have aggravated the shortcomings. Each of them increased the demand on the limited supply of addresses, often in ways unanticipated by the original designers of the network.

### Mobile devices

As IPv4 increasingly became the *de facto* standard for networked digital communication, the cost of embedding substantial computing power into hand-held devices dropped. Mobile phones have become viable Internet hosts. New specifications of 4G devices require IPv6 addressing.

### Always-on connections

Throughout the 1990s, the predominant mode of consumer Internet access was telephone modem dial-up. The rapid growth of the dial-up networks increased address consumption rates, although it was common that the modem pools, and as a result, the pool of assigned IP addresses, were shared amongst a larger customer base. By 2007, however, broadband Internet access had begun to exceed 50% penetration in many markets.<sup>[11]</sup> Broadband connections are always active, as the gateway devices (routers, broadband modems) are rarely turned off, so that the address uptake by Internet service providers continued at an accelerating pace.

### Internet demographics

There are hundreds of millions of households in the developed world. In 1990, only a small fraction of these had Internet connectivity. Just 15 years later, almost half of them had persistent broadband connections.<sup>[12]</sup> The many new Internet users in countries such as China and India are also driving address exhaustion.

### Inefficient address use

Organizations that obtained IP addresses in the 1980s were often allocated far more addresses than they actually required, because the initial classful network allocation method was inadequate to reflect reasonable usage. For example, large companies or universities were assigned class A address blocks with over 16 million IPv4 addresses each, because the next smaller allocation unit, a class B block with 65536 addresses, was too small for their intended deployments.

Many organizations continue to utilize public IP addresses for devices not accessible outside their local network. From a global address allocation viewpoint, this is inefficient in many cases, but scenarios exist where this is preferred in the organizational network implementation strategies.

Due to inefficiencies caused by subnetting, it is difficult to use all addresses in a block. The host-density ratio, as defined in RFC 3194, is a metric for utilization of IP address blocks, that is used in allocation policies.

## Early mitigation efforts

Efforts to delay address space exhaustion started with the recognition of the problem in the early 1990s, and include:

- Use of network address translation (NAT), in which many computers share one IP address, but which makes the computers behind the NAT unaddressable from the outside, breaking end-to-end connectivity
- Use of private network addressing<sup>[13]</sup>
- Name-based virtual hosting of web sites
- Tighter control by regional Internet registries on the allocation of addresses to local Internet registries
- Network renumbering and subnetting to reclaim large blocks of address space allocated in the early days of the Internet, when the Internet used inefficient classful network addressing

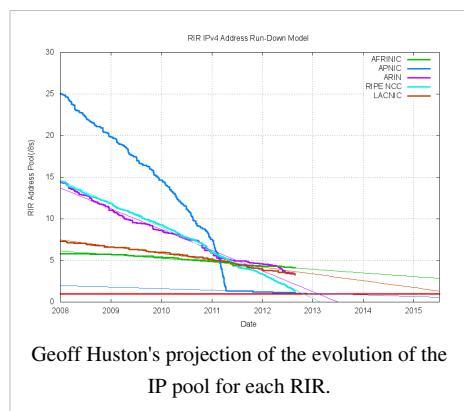
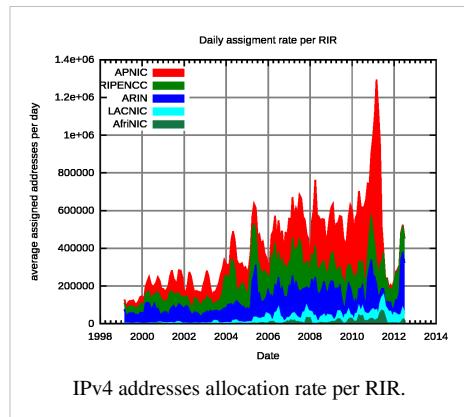
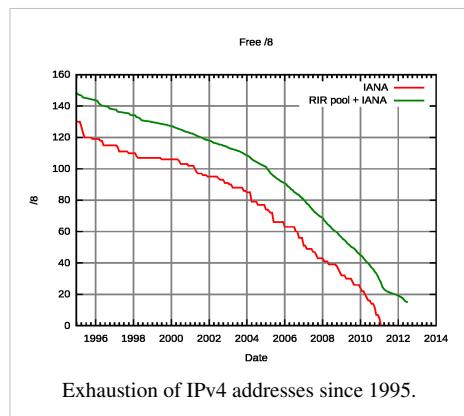
## Exhaustion dates and impact

On 31 January 2011, the last two unreserved IANA /8 address blocks were allocated to APNIC according to RIR request procedures. This left five reserved but unallocated /8 blocks.<sup>[4][14][15]</sup> In accord with ICANN policies, IANA proceeded to allocate one of those five /8s to each RIR, exhausting the IANA pool,<sup>[16]</sup> at a ceremony and press conference on 3 February 2011.

The various legacy address blocks with administration historically split among the RIRs were distributed to the RIRs in February 2011.<sup>[17]</sup>

APNIC was the first regional Internet Registry to run out of freely allocated IPv4 addresses, on 15 April 2011. This date marked the point where everybody who needed an IPv4 address could not be guaranteed to have one allocated. As a consequence of this exhaustion, end-to-end connectivity as required by specific applications will not be universally available on the Internet until IPv6 is fully implemented. However, IPv6 hosts cannot directly communicate with IPv4 hosts, and have to communicate using special gateway services. This means that general-purpose computers must still have IPv4 access, for example through NAT64, in addition to the new IPv6 address, which is more effort than just supporting IPv4 or IPv6. The demand for IPv6 is expected to ramp up to pervasiveness over three to four years.<sup>[18]</sup>

In early 2011, only 16–26% of computers were latent IPv6 capable, while only 0.2% prefer IPv6 addressing<sup>[19]</sup> many using transition methods such as Teredo tunneling.<sup>[20]</sup> About 0.15% of the top million websites are IPv6 accessible.<sup>[21]</sup> Complicating matters, 0.027% to 0.12% of visitors cannot reach dual-stack sites,<sup>[22][23]</sup> but a larger percentage (0.27%) cannot reach IPv4-only sites.<sup>[24]</sup> IPv4 exhaustion mitigation technologies include IPv4 address sharing to access IPv4 content, IPv6 dual-stack implementation, protocol translation to access IPv4 and IPv6-addressed content, and bridging and tunneling to bypass single protocol routers. Early signs of accelerated IPv6 adoption after IANA exhaustion are evident.<sup>[25]</sup>



## Regional exhaustion

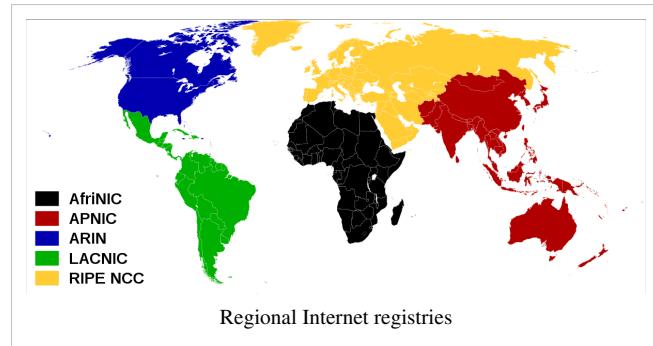
APNIC was the first RIR to restrict allocations to 1024 addresses for each member due to its stock reaching critical levels of 1 /8 at 14 April 2011.<sup>[4][26][27][28][29][30]</sup> The APNIC RIR is responsible for address-allocation in the area where the internet is growing the quickest with emerging markets like China and India.

RIPE NCC, the regional Internet registry for Europe, is expected to be the next RIR after APNIC to run

out of allocatable IPv4 addresses. This exhaustion is expected in the middle of 2012 according to Geoff Huston's projection. The exhaustion may occur sooner, depending on whether RIPE NCC experiences a last minute run on IPv4 addresses like the one seen at APNIC, and on whether LIRs which would normally have requested addresses from APNIC will now request addresses from RIPE NCC ("RIR shopping"). Starting 1 July 2010, RIPE has also been providing LIRs with addresses for progressively smaller periods of time, only providing addresses for up to 3 months of expected usage from 1 July 2011.<sup>[31]</sup>

Other RIRs are expected to exhaust within half a year to several years.<sup>[32]</sup>

After IANA exhaustion, IPv4 address space requests are subject to additional restrictions at ARIN,<sup>[33]</sup> but allocation policy is still largely unchanged. APNIC, LACNIC, and RIPE NCC are reserving the last obtained block for IPv6 transition, following special endgame set-aside policies.



### Impact of APNIC RIR exhaustion and LIR exhaustion

Systems that require inter-continental connectivity will have to deal with exhaustion mitigation already due to APNIC exhaustion. At APNIC, existing LIRs could apply for twelve months stock before exhaustion when they were using more than 80% of allocated space allocated to them.<sup>[34]</sup> Since 15 April 2011, the date when APNIC reached its last /8 block, each (current or future) member will only be able to get one allocation of 1024 addresses (a /22 block) once.<sup>[35][36]</sup> As the slope of the APNIC pool line on the "Geoff Huston's projection of the evolution of the IP pool for each RIR" chart to the right shows, the last /8 block would have been emptied within one month without this policy. By APNIC policy, each current or future member can receive only one /22 block from this last /8 (there are 16384 /22 blocks in the last /8 block). Since there are around 3000 current APNIC members, and around 300 new APNIC members each year, APNIC expects this last /8 block to last for many years.<sup>[37]</sup>

The 1024 addresses in the /22 block can be used by APNIC members to supply NAT44 or NAT64 as a service on an IPv6 network. However at a new large ISP, 1024 IPv4 addresses might not be enough to provide IPv4 connectivity to all the customers due to the limited number of ports available per IPv4 address.<sup>[38]</sup>

The Regional Internet Registries (RIR's) for Asia (APNIC) and North America have a policy called the Inter-RIR IPv4 Address Transfer Policy which allows IPv4 addresses to be transferred from North America to Asia.<sup>[39][40]</sup> The ARIN policy will receive final ratification on 16 November 2011.

IPv4 broker businesses have been established to facilitate these transfers.

### Notable exhaustion advisories

Estimates of the time of complete IPv4 address exhaustion varied widely in the early 2000s. In 2003, Paul Wilson (director of APNIC) stated that, based on then-current rates of deployment, the available space would last for one or two decades.<sup>[41]</sup> In September 2005, a report by Cisco Systems suggested that the pool of available addresses would deplete in as little as 4 to 5 years.<sup>[42]</sup> In the last year before exhaustion, IPv4 allocations were accelerating, resulting in exhaustion trending to earlier dates.

- On 21 May 2007, the American Registry for Internet Numbers (ARIN), the Anglo-American RIR, advised the Internet community that due to the expected exhaustion in 2010, "migration to IPv6 numbering resources is necessary for any applications which require ongoing availability from ARIN of contiguous IP numbering resources".<sup>[43]</sup> "Applications" include general connectivity between devices on the Internet, as some devices only have an IPv6 address allocated.
- On 20 June 2007, the Latin American and Caribbean Internet Addresses Registry (LACNIC), advised "preparing its regional networks for IPv6" by 1 January 2011, for the exhaustion of IPv4 addresses "in three years time".<sup>[44]</sup>
- On 26 June 2007, the Asia-Pacific Network Information Centre (APNIC), the RIR for the Pacific and Asia, endorsed a statement by the Japan Network Information Center (JPNIC) that to continue the expansion and development of the Internet a move towards an IPv6-based Internet is advised. This, with an eye on the expected exhaustion around 2010, will create a great restriction on the Internet.<sup>[45][46]</sup>
- On 26 October 2007, the Réseaux IP Européens Network Coordination Centre (RIPE NCC), the RIR for Europe, the Middle East, and parts of Central Asia, endorsed a statement<sup>[47]</sup> by the RIPE community urging "the widespread deployment of IPv6 be made a high priority by all stakeholders".
- On 15 April 2009, ARIN sent a letter to all CEO/Executives of companies who have IPv4 addresses allocated informing them that ARIN expects the IPv4 space will be depleted within the next two years.<sup>[48]</sup>
- In May 2009, the RIPE NCC launched IPv6ActNow.org<sup>[49]</sup> to help explain "IPv6 in terms everyone can understand and providing a variety of useful information aimed at promoting the global adoption of IPv6".
- On 25 August 2009, ARIN announced a joint series event in the Caribbean region to push for the implementation of IPv6. ARIN reported at this time that less than 10.9% of IPv4 address space is remaining.<sup>[50]</sup>
- World IPv6 Day was an event sponsored and organized by the Internet Society and several large content providers to test public IPv6 deployment. It started at 00:00 UTC on 8 June 2011 and ended at 23:59 the same day. The test primarily consisted of websites publishing AAAA records, allowing IPv6 capable hosts to connect to these sites using IPv6, and for misconfigured networks to be corrected.

## Post-exhaustion mitigation

By 2008 policy planning for the end-game and post-exhaustion era was underway.<sup>[51]</sup> Several proposals have been discussed to delay shortages of IPv4 addresses:

### Reclamation of unused IPv4 space

Before and during the time when classful network design was still used as allocation model, large blocks of IP addresses were allocated to some organizations. Since the use of Classless Inter-Domain Routing (CIDR) the Internet Assigned Numbers Authority (IANA) could potentially reclaim these ranges and reissue the addresses in smaller blocks. ARIN, RIPE NCC and APNIC have a transfer policy, such that addresses can get returned, with the purpose to be reassigned to a specific recipient.<sup>[52][53][54]</sup> However, it can be expensive in terms of cost and time to renumber a large network, so these organizations will likely object, with legal conflicts possible. However, even if all of these were reclaimed, it would only result in postponing the date of address exhaustion.

Similarly, IP address blocks have been allocated to entities that no longer exist and some allocated IP address blocks or large portions of them have never been used. No strict accounting of IP address allocations has been undertaken, and it would take quite a bit of effort to track down which addresses really are unused, as many are only in use on intranets.

Some address space that was previously reserved by IANA has been added to the available pool. There have been proposals to use the class E network range of IPv4 addresses,<sup>[55][56]</sup> but many computer and router operating systems and firmware do not allow the use of these addresses.<sup>[42][57][58][59]</sup> For this reason, the proposals have sought not to designate the class E space for public assignment, but instead propose to permit its private use for networks that require more address space than is currently available through RFC 1918.

Several organizations have returned large blocks of IP addresses. Notably, Stanford University relinquished their Class A IP block in 2000, making 16 million IP addresses available.<sup>[60]</sup> Other organizations that have done so include the United States Department of Defense, BBN Technologies, and Interop.<sup>[61]</sup>

## Markets in IP addresses

The creation of markets to buy and sell IPv4 addresses has been considered to be a solution to the problem of IPv4 scarcity and a means of redistribution. The primary benefits of an IPv4 address market are that it allows buyers to maintain undisrupted local network functionality.<sup>[62][63]</sup> IPv6 adoption, while in progress, is currently still in early stages.<sup>[64]</sup> It requires a significant investment of resources, and poses incompatibility issues with IPv4, as well as certain security and stability risks.<sup>[65][66]</sup>

- According to some research, IPv6 traffic over 2011 has accounted for less than 0.3% of all the Internet traffic, regardless of the source. Also, very few ISPs currently deploy IPv6 to the consumer market, so it is not necessary to reach more consumers.<sup>[67]</sup>
- The creation of a market in IPv4 addresses would only delay the practical exhaustion of the IPv4 address space for a relatively short time, since the public Internet is still growing.
- The concept of legal ownership of IP addresses as property is explicitly denied by ARIN and RIPE NCC policy documents and by the ARIN Registration Services Agreement. Nor is it clear in which country's legal system the lawsuits would be resolved.
- Ad-hoc trading in addresses could lead to fragmented patterns of routing that could expand the global routing table.
- Microsoft bought 666,624 IPv4 addresses from Nortel's liquidation sale for 7.5 million dollars in a deal brokered by Addrex.<sup>[68][69]</sup> Before exhaustion, Microsoft could have obtained addresses from ARIN without charge, provided that, as per ARIN policy, Microsoft could present ARIN with a need for them.<sup>[70]</sup> The success of this transfer was contingent on Microsoft successfully presenting ARIN with such a justification. The purchase provided Microsoft with a supply that was sufficient for their claimed needs for growth over the next 12 months, rather than for a 3-months' period as is normally requested from ARIN.<sup>[71]</sup>

## Transition mechanisms

As IPv4 addresses run out, some ISPs will not be able to provide globally routable IPv4 addresses to all their customers. Nevertheless those customers are likely to require access to servers that only have IPv4 addresses. Therefore, ISPs may have to provide a mechanism that allows those customers access to the IPv4 Internet. Several technologies have been developed for providing this IPv4 service over an IPv6 access network.

In ISP-level IPv4 NAT, ISPs may implement IPv4 network address translation within their networks and allocate private IPv4 addresses to customers. This approach has the advantage of allowing the customer to keep using their existing hardware. This has been successfully implemented in some countries, e.g., Russia, where many broadband providers use Carrier-grade NAT, and offer publicly routable IPv4 address at an additional cost.

However the allocation of private IPv4 addresses to customers may conflict with private IP allocations on the customer networks. Furthermore, very large ISPs may have to divide their network into subnets to allow them to reuse private IPv4 addresses, complicating network administration. There are also concerns that features of consumer-grade NAT such as DMZs, STUN, UPnP and application-level gateways might not be available at the ISP level. ISP-level NAT is likely to result in double NAT which is likely to further complicate the use of such mechanisms.

NAT64 translates IPv6 requests from clients to IPv4 requests. This avoids the need to provision any IPv4 addresses to clients and allows clients that only support IPv6 to access IPv4 resources. However this approach requires modifying DNS replies (DNS64) and cannot support IPv4-only client devices.

DS-Lite (Dual-Stack Light) uses tunnels from the customer premises equipment to a network address translator at the ISP.<sup>[72]</sup> The consumer premise equipment encapsulates the IPv4 packets in an IPv6 wrapper and sends them to a host known as the *AFTR element*. The AFTR element de-encapsulates the packets and performs network address translation before sending them to the public Internet. The NAT in the AFTR uses the IPv6 address of the client in its NAT mapping table. This means that different clients can use the same private IPv4 addresses, therefore avoiding the need for allocating private IPv4 IP addresses to customers or using multiple NATs.

Address plus Port allows stateless sharing of public IP addresses based on TCP/UDP port numbers. Each node is allocated both an IPv4 address and a range of port numbers to use. The technique avoids the need for stateful address translation mechanisms in the core of the network, thus leaving end users in control of their own address translation.

## Long-term solution

The deployment of IPv6 is the only available solution to the IPv4 address shortage.<sup>[5]</sup> IPv6 is endorsed and implemented by all Internet technical standards bodies and network equipment vendors. It encompassed many design improvements, including the replacement of the 32-bit IPv4 address format with a 128-bit address for a capacity of about  $3.4 \times 10^{38}$  addresses. IPv6 has been in active production deployment since June 2006, after organized worldwide testing and evaluation in the 6bone project ceased.

## References

- [1] Smith, Lucie; Lipner, Ian (3 February 2011). "Free Pool of IPv4 Address Space Depleted" (<http://www.nro.net/news/ipv4-free-pool-depleted>). Number Resource Organization. . Retrieved 3 February 2011.
- [2] Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied (<http://www.icann.org/en/news/releases/release-03feb11-en.pdf>), Major Announcement Set on Dwindling Pool of Available IPv4 Internet Addresses (<http://www.icann.org/en/news/advisories/advisory-01feb11-en.pdf>)
- [3] ICANN,nanog mailing list. "Five /8s allocated to RIRs – no unallocated IPv4 unicast /8s remain" (<http://mailman.nanog.org/pipermail/nanog/2011-February/032107.html>). .
- [4] Huston, Geoff. "IPv4 Address Report, daily generated" (<http://www.potaroo.net/tools/ipv4/index.html>). . Retrieved 16 January 2011.
- [5] "Two /8s allocated to APNIC from IANA" (<http://www.apnic.net/publications/news/2011/delegation>). APNIC. 1 February 2010. . Retrieved 3 February 2011.
- [6] "APNIC IPv4 Address Pool Reaches Final /8" (<http://www.apnic.net/publications/news/2011/final-8>). APNIC. 15 April 2011. . Retrieved 15 April 2011.
- [7] RFC 4632
- [8] Niall Richard Murphy, David Malone (2005). *IPv6 network administration*. O'Reilly Media, Inc.. pp. xvii–xix. ISBN 0-596-00934-8.
- [9] Mark Townsley (21 January 2011). "World IPv6 Day: Working Together Towards a New Internet Protocol" (<http://blogs.cisco.com/news/world-ipv6-day-working-together-towards-a-new-internet-protocol/>). .
- [10] S.H. Gunderson (2008-10). "Global IPv6 Statistics – Measuring the current state of IPv6 for ordinary users" ([http://www.ripe.net/ripe/meetings/ripe-57/presentations/Colitti-Global\\_IPv6\\_statistics\\_-\\_Measuring\\_the\\_current\\_state\\_of\\_IPv6\\_for\\_ordinary\\_users\\_.7gzD.pdf](http://www.ripe.net/ripe/meetings/ripe-57/presentations/Colitti-Global_IPv6_statistics_-_Measuring_the_current_state_of_IPv6_for_ordinary_users_.7gzD.pdf)) (PDF). . Retrieved 10 November 2010.
- [11] Ferguson, Tim (18 February 2007). "Broadband adoption passes halfway mark in U.S." ([http://www.news.com/Broadband-adoption-passes-halfway-mark-in-U.S./2110-1034\\_3-6160422.html](http://www.news.com/Broadband-adoption-passes-halfway-mark-in-U.S./2110-1034_3-6160422.html)). CNET News.com. . Retrieved 10 November 2010.
- [12] "Projections of the Number of Households and Families in the United States: 1995 to 2010" (<http://www.census.gov/prod/1/pop/p25-1129.pdf>) (PDF). 1996-04. . Retrieved 10 November 2010.
- [13] RFC 1918 Section 4
- [14] IANA. "IANA IPv4 Address Space Registry" (<http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.txt>). IANA IPv4 Address Space Registry. . Retrieved 31 January 2011.
- [15] Stephen Lawson (31 January 2011). "Address allocation kicks off IPv4 endgame" ([http://www.computerworld.com/s/article/9207438/Address\\_allocation\\_kicks\\_off\\_IPv4\\_endgame](http://www.computerworld.com/s/article/9207438/Address_allocation_kicks_off_IPv4_endgame)). Computerworld. .
- [16] "Global Policy for the Allocation of the Remaining IPv4 Address Space" (<http://www.icann.org/en/general/allocation-remaining-ipv4-space.htm>). . Retrieved 1 February 2011.
- [17] "The IPv4 Depletion site » Blog Archive » Status of the various pool" (<http://www.ipv4depletion.com/?p=524>). Ipv4depletion.com. 3 December 2010. . Retrieved 2 December 2011.
- [18] "www.fix6.net" (<http://www.fix6.net/archives/2010/11/24/ipv6-and-transitional-myths/>). www.fix6.net. 24 November 2010. . Retrieved 3 February 2011.
- [19] "ISP Column - May 2011" (<http://www.potaroo.net/ispcol/2011-04/teredo.html>). Potaroo.net. . Retrieved 2 December 2011.

- [20] [http://www.apricot-apan.asia/\\_\\_data/assets/pdf\\_file/0012/31314/2011-02-23-dualstack-geoff.pdf](http://www.apricot-apan.asia/__data/assets/pdf_file/0012/31314/2011-02-23-dualstack-geoff.pdf)
- [21] "IPv6 Measurements – A Compilation — RIPE Labs" (<http://labs.ripe.net/Members/mirjam/content-ipv6-measurement-compilation>). RIPE Labs.ripe.net. . Retrieved 2 December 2011.
- [22] "IPV6 Test – Introductie" (<http://ipv6test.max.nl>). Ipv6test.max.nl. . Retrieved 2 December 2011.
- [23] [http://www.nanog.org/meetings/nanog51/presentations/Tuesday/Y\\_world\\_ipv6\\_day\\_v2.pdf](http://www.nanog.org/meetings/nanog51/presentations/Tuesday/Y_world_ipv6_day_v2.pdf)
- [24] "ISP Column – April 2010" (<http://www.potaroo.net/ispcol/2010-04/ipv6-measure.html>). Potaroo.net. . Retrieved 2 December 2011.
- [25] Carolyn Duffy Marsan (7 February 2011). "Suddenly everybody's selling IPv6" (<http://www.networkworld.com/news/2011/020711-address-depletion-ipv6.html>). Network World. .
- [26] "APNIC's IPv4 pool usage" (<http://www.apnic.net/community/ipv4-exhaustion/graphical-information>). Apnic.net. . Retrieved 2 December 2011.
- [27] APNIC IPv4 Address Pool Reaches Final /8 (<http://mailman.apnic.net/mailings-lists/apnic-announce/archive/2011/04/msg00002.html>) [Apnic-announce], 15 April 2011
- [28] <http://www.potaroo.net/tools/ipv4/fig27h.png>
- [29] <http://www.potaroo.net/presentations/2011-02-25-movie.pdf>
- [30] <http://www.tndh.net/~tony/ietf/IPv4-rir-pools-zoom.jpg>
- [31] "IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region - section "5.0 Policies and Guidelines for Allocations"" (<http://www.ripe.net/ripe/docs/ripe-530#---policies-and-guidelines-for-allocations>). RIPE. .
- [32] "Registry Exhaustion Dates" (<http://www.potaroo.net/ispcol/2011-02/rir.pdf>). . Retrieved 4 April 2011.
- [33] "information on ARIN website" ([https://www.arin.net/resources/request/ipv4\\_depletion.html](https://www.arin.net/resources/request/ipv4_depletion.html)). Arin.net. . Retrieved 3 February 2011.
- [34] "APNIC – Policies for IPv4 address space management in the Asia Pacific region" (<http://www.apnic.net/policy/add-manage-policy#9.4>). Apnic.net. . Retrieved 2 December 2011.
- [35] "APNIC – Policies for IPv4 address space management in the Asia Pacific region" (<http://www.apnic.net/policy/add-manage-policy#9.10>). Apnic.net. . Retrieved 2 December 2011.
- [36] "APNIC – IPv4 exhaustion details" (<http://www.apnic.net/community/ipv4-exhaustion/ipv4-exhaustion-details>). Apnic.net. 3 February 2011.. Retrieved 2 December 2011.
- [37] "IPv4 exhaustion details" (<http://www.apnic.net/community/ipv4-exhaustion/ipv4-exhaustion-details>). APNIC. .
- [38] "No more addresses: Asia-Pacific region IPv4 well runs dry" (<http://arstechnica.com/tech-policy/news/2011/04/no-more-addresses-asia-pacific-region-ipv4-well-runs-dry.ars>). Arstechnica. 15 April 2011.. Retrieved 16 April 2011.
- [39] Tomohiro Fujisaki (24 February 2011). "prop-095-v003: Inter-RIR IPv4 address transfer proposal" ([http://www.apnic.net/\\_\\_data/assets/text\\_file/0017/31607/prop-095-v003.txt](http://www.apnic.net/__data/assets/text_file/0017/31607/prop-095-v003.txt)). . Retrieved 9 November 2011.
- [40] "Draft Policy ARIN-2011-1: ARIN Inter-RIR Transfers" ([https://www.arin.net/policy/proposals/2011\\_1.html](https://www.arin.net/policy/proposals/2011_1.html)). 14 October 2011.. Retrieved 9 November 2011.
- [41] Exec: No shortage of Net addresses ([http://news.zdnet.com/2100-1009\\_22-1020653.html](http://news.zdnet.com/2100-1009_22-1020653.html)) By John Lui, CNETAsia
- [42] Hain, Tony. "A Pragmatic Report on IPv4 Address Space Consumption" ([http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ijpj\\_8-3/ipv4.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ijpj_8-3/ipv4.html)). . Retrieved 14 November 2007.
- [43] "ARIN Board Advises Internet Community on Migration to IPv6" (<https://www.arin.net/announcements/2007/20070521.html>) (Press release). American Registry for Internet Numbers (ARIN). 21 May 2007.. Retrieved 1 July 2007.
- [44] "LACNIC announces the imminent depletion of the IPv4 addresses" ([http://lacnic.net/en/anuncios/2007\\_agotamiento\\_ipv4.html](http://lacnic.net/en/anuncios/2007_agotamiento_ipv4.html)) (Press release). Latin American and Caribbean Internet Addresses Registry (LACNIC). 21 June 2007.. Retrieved 1 July 2007.
- [45] "JPNIC releases statement on IPv4 consumption" (<http://www.apnic.net/publications/news/2007/jpnic-ipv4>) (Press release). Asia-Pacific Network Information Centre (APNIC). 26 June 2007.. Retrieved 1 July 2007.
- [46] "About IPv4 address exhaustion in Internet Registries" (<http://www.nic.ad.jp/ja/ip/ipv4pool/ipv4pool-JPNIC-070619.pdf>) (in Japanese) (PDF) (Press release). Japan Network Information Center (JPNIC). 19 June 2007.. Retrieved 1 July 2007.
- [47] "RIPE 55 – Meeting Report" (<http://www.ripe.net/ripe/meetings/ripe-55/report.html>). RIPE NCC. 26 October 2007.. Retrieved 2 February 2011.
- [48] "Notice of Internet Protocol version 4 (IPv4) Address Depletion" ([https://www.arin.net/knowledge/about\\_resources/ceo\\_letter.pdf](https://www.arin.net/knowledge/about_resources/ceo_letter.pdf)) (PDF). . Retrieved 3 February 2011.
- [49] <http://ipv6actnow.org>
- [50] White, Lauren (25 August 2009). "ARIN and Caribbean Telecommunications Union Host Premier Internet Community Meeting" (<http://www.businesswire.com/news/google/20090825005958/en>). Archived from the original ([http://www.businesswire.com/portal/site/google/?ndmViewId=news\\_view&newsId=20090825005958&newsLang=en](http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20090825005958&newsLang=en)) on 27 August 2009.. Retrieved 27 August 2009. ""The global Internet community is playing a crucial role in the effort to raise awareness of IPv4 depletion and the plan to deploy IPv6, as only 10.9% of IPv4 address space currently remains.""
- [51] "Proposed Global Policy for the Allocation of the Remaining IPv4 Address Space" (<http://www.ripe.net/ripe/policies/proposals/2008-03.html>). RIPE NCC. 3 March 2008. . Retrieved 10 November 2010.
- [52] "APNIC transfer policy" (<http://www.apnic.net/policy/transfer-policy>). Apnic.net. 10 February 2010.. Retrieved 3 February 2011.
- [53] "ARIN transfer policy" (<https://www.arin.net/resources/transfers/index.html>). Arin.net. . Retrieved 3 February 2011.
- [54] "Ripe FAQ" (<http://www.ripe.net/info/faq/IPv6-deployment.html#2>). Ripe.net. . Retrieved 3 February 2011.

- [55] Wilson, Paul; Michaelson, George; Huston, Geoff. "Redesignation of 240/4 from "Future Use" to "Limited Use for Large Private Internets" (expired draft)" (<http://tools.ietf.org/html/draft-wilson-class-e>). . Retrieved 5 April 2010.
- [56] V. Fuller, E. Lear, D. Meyer (24 March 2008). "Reclassifying 240/4 as usable unicast address space (expired draft)" (<http://tools.ietf.org/html/draft-fuller-240space>). IETF. . Retrieved 10 November 2010.
- [57] "Address Classes" ([http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/cnet/cnbb\\_tcp\\_zrnh.mspx?mfr=true](http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/cnet/cnbb_tcp_zrnh.mspx?mfr=true)). *Windows 2000 Resource Kit*. Microsoft. . Retrieved 14 November 2007.
- [58] van Beijnum, Iljitsch. "IPv4 Address Consumption" ([http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_10-3/103\\_addr-cons.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-3/103_addr-cons.html)). . Retrieved 14 November 2007.
- [59] "TCP/IP Overview" (<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwhubs/starvwug/83428.htm#xtocid74886>). Cisco Systems, Inc. . Retrieved 14 November 2007.
- [60] Marsan, Carolyn. "Stanford move rekindles 'Net address debate" (<http://www.networkworld.com/news/2000/0124ipv4.html>). Network World. . Retrieved 29 June 2010.
- [61] "ARIN Recognizes Interop for Returning IPv4 Address Space" (<https://www.arin.net/announcements/2010/20101020.html>). Arin.net. 20 October 2010. . Retrieved 3 February 2011.
- [62] Phil Lodico (15 September 2011). "Pssst! Rare IPv4 Addresses For Sale! Get Them While You Can!" (<http://www.forbes.com/sites/ciocentral/2011/09/15/pssst-rare-ipv4-addresses-for-sale-get-them-while-you-can/>). .
- [63] KRISTINA BJORAN (27 July 2011). "The State of the Internet: IPv4 Won't Die" (<http://www.technologyreview.com/blog/editors/27038/>). .
- [64] Steve Wexler (18 October 2011). "IPv6: Unstoppable Force Meets Immovable Object" (<http://www.networkcomputing.com/ipv6-tech-center/231900971>). .
- [65] David Braue (20 October 2011). "IPv6 will change network attack surface, albeit slowly: Huston" ([http://www.cso.com.au/article/404785/ipv6\\_will\\_change\\_network\\_attack\\_surface\\_albeit\\_slowly\\_huston/](http://www.cso.com.au/article/404785/ipv6_will_change_network_attack_surface_albeit_slowly_huston/)). .
- [66] Elizabeth Harrin (22 September 2011). "IPv6 Will Cause Some Security Headaches" (<http://www.esecurityplanet.com/network-security/ipv6-will-cause-some-security-headaches.html>). .
- [67] Ken Salchow (6 September 2011). "IPv6 migration: Do it for the right reasons" ([http://www.computerworld.com/s/article/9219738/IPv6\\_migration\\_Do\\_it\\_for\\_the\\_right\\_reasons?taxonomyId=16](http://www.computerworld.com/s/article/9219738/IPv6_migration_Do_it_for_the_right_reasons?taxonomyId=16)). .
- [68] Chloe Albanesius (25 March 2011). "Microsoft Spends \$7.5M on 666K Nortel IPv4 Addresses" (<http://www.pcmag.com/article2/0,2817,2382616,00.asp>). PC Magazine. .
- [69] Kevin Murphy (24 March 2011). "Microsoft spends \$7.5 million on IP addresses" (<http://domainincite.com/microsoft-spends-7-5-million-on-ip-addresses/>). Domain Incite. .
- [70] "Resource Transfers: Returning Unneeded IPv4 Address Space" (<https://www.arin.net/resources/transfers/index.html>). ARIN. .
- [71] Jaikumar Vijayan (25 March 2011). "IPv4 address transfers must meet policy, ARIN chief says" ([http://www.computerworld.com/s/article/9215091/IPv4\\_address\\_transfers\\_must\\_meet\\_policy\\_ARIN\\_chief\\_says](http://www.computerworld.com/s/article/9215091/IPv4_address_transfers_must_meet_policy_ARIN_chief_says)). .
- [72] RFC 6333 - Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion

## External links

- Official current state of IPv4 /8 allocations, as maintained by IANA (<http://www.iana.org/assignments/ipv4-address-space>)
- IPv6.com – Knowledge Center for Next Generation Internet IPv6 (<http://www.ipv6.com>)
- ICANN recovers Large Block of Internet Addresses (14.0.0.0/8) (<http://www.icann.org/en/announcements/announcement-2-10feb08.htm>) 2008-02-10
- Global Policy Proposal for Remaining IPv4 Address Space – Background Report (<http://www.icann.org/en/announcements/proposal-ipv4-report-29nov07.htm>) 2008-09-08
- potaroo.net: IPv4 Address Report with countdown (<http://www.potaroo.net/tools/ipv4/>)
- RIR IPv4 status: APNIC (<http://www.apnic.net/community/ipv4-exhaustion/graphical-information>) RIPE (<http://www.ripe.net/internet-coordination/ipv4-exhaustion/ipv4-available-pool-graph>)

# IPv6

**IPv6 (Internet Protocol version 6)** is a revision of the Internet Protocol (IP) developed by the Internet Engineering Task Force (IETF). IPv6 is intended to succeed IPv4, which is the dominant communications protocol for most Internet traffic as of 2012.<sup>[1]</sup> IPv6 was developed to deal with the long-anticipated problem of IPv4 running out of addresses. IPv6 implements a new addressing system that allows for far more addresses to be assigned than with IPv4.

Each device on the Internet, such as a computer or mobile telephone, must be assigned an IP address in order to communicate with other devices. With the ever-increasing number of new devices being connected to the Internet, there is a need for more addresses than IPv4 can accommodate. IPv6 uses 128-bit addresses, allowing for  $2^{128}$ , or approximately  $3.4 \times 10^{38}$  addresses — more than  $7.9 \times 10^{28}$  times as many as IPv4, which uses 32-bit addresses. IPv4 allows for only 4,294,967,296 unique addresses worldwide (or less than one address per person alive in 2012), but IPv6 allows for around  $4.8 \times 10^{28}$  addresses per person — a number unlikely ever to run out.

IPv6 addresses, as commonly displayed to users, consist of eight groups of four hexadecimal digits separated by colons, for example 2001:0db8:85a3:0042:0000:8a2e:0370:7334.

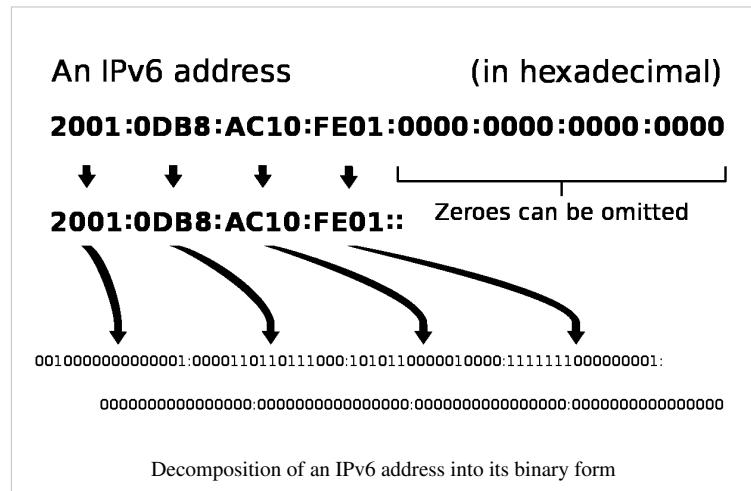
The deployment of IPv6 is accelerating, with a World IPv6 Launch having taken place on 6 June 2012, in which major internet service providers, especially in countries that had been lagging in IPv6 adoption, deployed IPv6 addresses to portions of their users.<sup>[2]</sup> Data from Arbor Networks showed a peak of 0.2% of Internet traffic on IPv6 during the launch.<sup>[3]</sup>

## Technical definition

IPv6, like the most commonly used IPv4 (as of 2012), is an Internet-layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks. It is described in Internet standard document RFC 2460, published in December 1998.<sup>[4]</sup> In addition to offering more addresses, IPv6 also implements features not present in IPv4. It simplifies aspects of address assignment (stateless address autoconfiguration), network renumbering and router announcements when changing network

connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from link-layer media addressing information (MAC address). Network security is also integrated into the design of the IPv6 architecture, including the option of IPsec.

IPv6 does not implement interoperability features with IPv4, but essentially creates a parallel, independent network. Exchanging traffic between the two networks requires special translator gateways, but this is not generally required, since most computer operating systems and software implement both protocols for transparent access to both networks, either natively or using a tunneling protocol like 6to4, 6in4, or Teredo.



## Motivation and origin

### IPv4

Internet Protocol Version 4 (IPv4) was the first publicly used version of the Internet Protocol. IPv4 addresses are typically displayed as four numbers, each in the range 0 to 255, or 8 bits per number, for a total of 32 bits. Thus IPv4 provides an addressing capability of  $2^{32}$  or approximately 4.3 billion addresses. Address exhaustion was not initially a concern in IPv4 as this version was originally presumed to be an internal test within ARPA, and not intended for public use.

An IPv4 address (dotted-decimal notation)

**172 . 16 . 254 . 1**

**10101100 . 00010000 . 11111110 . 00000001**

**One byte =Eight bits**

**Thirty-two bits (4 x 8), or 4 bytes**

Decomposition of an IPv4 address to its binary value

The decision to put a 32-bit address

space on there was the result of a year's battle among a bunch of engineers who couldn't make up their minds about 32, 128, or variable-length. And after a year of fighting, I said—I'm now at ARPA, I'm running the program, I'm paying for this stuff, I'm using American tax dollars, and I wanted some progress because we didn't know if this was going to work. So I said: OK, it's 32-bits. That's enough for an experiment; it's 4.3 billion terminations. Even the Defense Department doesn't need 4.3 billion of everything and couldn't afford to buy 4.3 billion edge devices to do a test anyway. So at the time I thought we were doing an experiment to prove the technology and that if it worked we'd have opportunity to do a production version of it. Well, it just escaped! It got out and people started to use it, and then it became a commercial thing. So this [IPv6] is the production attempt at making the network scalable.

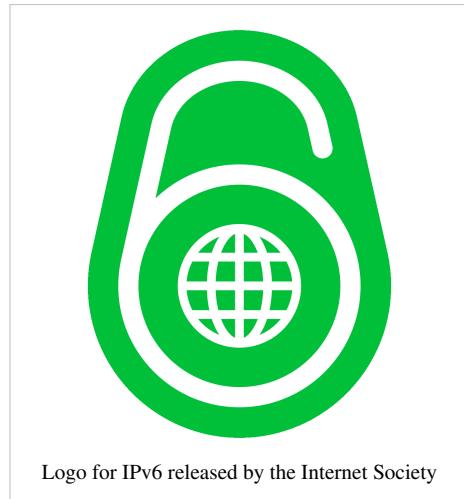
—Vint Cerf, Google IPv6 Conference 2008<sup>[5]</sup>

During the first decade of operation of the Internet (by the late 1980s), it became apparent that methods had to be developed to conserve address space. In the early 1990s, even after the redesign of the addressing system using a classless network model, it became clear that this would not suffice to prevent IPv4 address exhaustion, and that further changes to the Internet infrastructure were needed.<sup>[6]</sup>

The last available top-level (/8) blocks of 16 million IPv4 addresses were assigned in February 2011 by the Internet Assigned Numbers Authority (IANA) to the five Regional Internet registries (RIRs). However, many free addresses still remain within most assigned blocks, and each RIR will continue with standard address allocation policy until it is at its last /8 block. After that, only blocks of 1024 addresses (a /22) will be made available from the RIR to each Local Internet registry (LIR). As of February 2011, only the Asia-Pacific Network Information Centre (APNIC) had reached this stage.<sup>[7]</sup>

## Working-group proposal

By the beginning of 1992, several proposals appeared and by the end of 1992, the IETF announced a call for white papers.<sup>[8]</sup> In September 1993, the IETF created a temporary, ad-hoc *IP Next Generation* (IPng) area to deal specifically with IPng issues. The new area was led by Allison Mankin and Scott Bradner, and had a directorate with 15 engineers from diverse backgrounds for direction-setting and preliminary document review.<sup>[6][9]</sup> The working-group members were J. Allard (Microsoft), Steve Bellovin (AT&T), Jim Bound (Digital Equipment Corporation), Ross Callon (Wellfleet), Brian Carpenter (CERN), Dave Clark (MIT), John Curran (NEARNET), Steve Deering (Xerox), Dino Farinacci (Cisco), Paul Francis (NTT), Eric Fleischmann (Boeing), Mark Knopper (Ameritech), Greg Minshall (Novell), Rob Ullmann (Lotus), and Lixia Zhang (Xerox).



Logo for IPv6 released by the Internet Society

The Internet Engineering Task Force adopted the IPng model on July 25, 1994, with the formation of several IPng working groups.<sup>[6]</sup> By 1996, a series of RFCs was released defining Internet Protocol version 6 (IPv6), starting with RFC 1883. (Version 5 was used by the experimental Internet Stream Protocol.)

It is widely expected that the Internet will use IPv4 alongside IPv6 for the foreseeable future. IPv4-only and IPv6-only nodes cannot communicate directly, and need assistance from an intermediary gateway or must use other transition mechanisms.

## Exhaustion of IPv4 addresses

On February 3, 2011, in a ceremony in Miami, the Internet Assigned Numbers Authority (IANA) assigned the last batch of five /8 address blocks to the Regional Internet Registries,<sup>[10]</sup> officially depleting the global pool of completely fresh blocks of addresses.<sup>[11]</sup> Each /8 address block represents approximately 16.7 million possible addresses, for a total of over 80 million potential addresses combined.

At the time, it was anticipated that these addresses could well be fully consumed within three to six months at then-current rates of allocation.<sup>[12]</sup> APNIC was the first RIR to exhaust its regional pool on 15 April 2011, except for a small amount of address space reserved for the transition to IPv6, which will be allocated in a much more restricted way.<sup>[13]</sup>

In 2003, the director of Asia-Pacific Network Information Centre (APNIC), Paul Wilson, stated that, based on then-current rates of deployment, the available space would last for one or two decades.<sup>[14]</sup> In September 2005, a report by Cisco Systems suggested that the pool of available addresses would exhaust in as little as 4 to 5 years.<sup>[15]</sup> In 2008, a policy process started for the end-game and post-exhaustion era.<sup>[16]</sup> In 2010, a daily updated report projected the global address pool exhaustion by the first quarter of 2011, and depletion at the five regional Internet registries before the end of 2011.<sup>[17]</sup>

## Comparison to IPv4

IPv6 specifies a new packet format, designed to minimize packet header processing by routers.<sup>[4][18]</sup> Because the headers of IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable. However, in most respects, IPv6 is a conservative extension of IPv4. Most transport and application-layer protocols need little or no change to operate over IPv6; exceptions are application protocols that embed internet-layer addresses, such as FTP and NTPv3, where the new address format may cause conflicts with existing protocol syntax.

## Larger address space

The main advantage of IPv6 over IPv4 is its larger address space. The length of an IPv6 address is 128 bits, compared to 32 bits in IPv4.<sup>[4]</sup> The address space therefore has  $2^{128}$  or approximately  $3.4 \times 10^{38}$  addresses. By comparison, this amounts to approximately  $4.8 \times 10^{28}$  addresses for each of the seven billion people alive in 2011.<sup>[19]</sup> In addition, the IPv4 address space is poorly allocated, with approximately 14% of all available addresses utilized.<sup>[20]</sup> While these numbers are large, it wasn't the intent of the designers of the IPv6 address space to assure geographical saturation with usable addresses. Rather, the longer addresses simplify allocation of addresses, enable efficient route aggregation, and allow implementation of special addressing features. In IPv4, complex Classless Inter-Domain Routing (CIDR) methods were developed to make the best use of the small address space. The standard size of a subnet in IPv6 is  $2^{64}$  addresses, the square of the size of the entire IPv4 address space. Thus, actual address space utilization rates will be small in IPv6, but network management and routing efficiency is improved by the large subnet space and hierarchical route aggregation.

Renumbering an existing network for a new connectivity provider with different routing prefixes is a major effort with IPv4.<sup>[21][22]</sup> With IPv6, however, changing the prefix announced by a few routers can in principle renumber an entire network, since the host identifiers (the least-significant 64 bits of an address) can be independently self-configured by a host.<sup>[23]</sup>

## Multicasting

Multicasting, the transmission of a packet to multiple destinations in a single send operation, is part of the base specification in IPv6. In IPv4 this is an optional although commonly implemented feature.<sup>[24]</sup> IPv6 multicast addressing shares common features and protocols with IPv4 multicast, but also provides changes and improvements by eliminating the need for certain protocols. IPv6 does not implement traditional IP broadcast, i.e. the transmission of a packet to all hosts on the attached link using a special *broadcast address*, and therefore does not define broadcast addresses. In IPv6, the same result can be achieved by sending a packet to the link-local *all nodes* multicast group at address `ff02::1`, which is analogous to IPv4 multicast to address `224.0.0.1`. IPv6 also provides for new multicast implementations, including embedding rendezvous point addresses in an IPv6 multicast group address, which simplifies the deployment of inter-domain solutions.<sup>[25]</sup>

In IPv4 it is very difficult for an organization to get even one globally routable multicast group assignment, and the implementation of inter-domain solutions is very arcane.<sup>[26]</sup> Unicast address assignments by a local Internet registry for IPv6 have at least a 64-bit routing prefix, yielding the smallest subnet size available in IPv6 (also 64 bits). With such an assignment it is possible to embed the unicast address prefix into the IPv6 multicast address format, while still providing a 32-bit block, the least significant bits of the address, or approximately 4.2 billion multicast group identifiers. Thus each user of an IPv6 subnet automatically has available a set of globally routable source-specific multicast groups for multicast applications.<sup>[27]</sup>

## Stateless address autoconfiguration (SLAAC)

IPv6 hosts can configure themselves automatically when connected to a routed IPv6 network using the Neighbor Discovery Protocol via Internet Control Message Protocol version 6 (ICMPv6) router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; if configured suitably, routers respond to such a request with a router advertisement packet that contains network-layer configuration parameters.<sup>[23]</sup>

If IPv6 stateless address autoconfiguration is unsuitable for an application, a network may use stateful configuration with the Dynamic Host Configuration Protocol version 6 (DHCPv6) or hosts may be configured statically.

Routers present a special case of requirements for address configuration, as they often are sources for autoconfiguration information, such as router and prefix advertisements. Stateless configuration for routers can be achieved with a special router renumbering protocol.<sup>[28]</sup>

## Network-layer security

Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread deployment first in IPv4, into which it was back-engineered. Earlier, IPsec was an integral part of the base IPv6 protocol suite,<sup>[4][29]</sup> but has since been made optional.<sup>[30]</sup>

## Simplified processing by routers

In IPv6, the packet header and the process of packet forwarding have been simplified. Although IPv6 packet headers are at least twice the size of IPv4 packet headers, packet processing by routers is generally more efficient,<sup>[4][18]</sup> thereby extending the end-to-end principle of Internet design. Specifically:

- The packet header in IPv6 is simpler than that used in IPv4, with many rarely used fields moved to separate optional header extensions.
- IPv6 routers do not perform fragmentation. IPv6 hosts are required to either perform path MTU discovery, perform end-to-end fragmentation, or to send packets no larger than the IPv6 default minimum MTU size of 1280 octets.
- The IPv6 header is not protected by a checksum; integrity protection is assumed to be assured by both link-layer and higher-layer (TCP, UDP, etc.) error detection. UDP/IPv4 may actually have a checksum of 0, indicating no checksum; IPv6 requires UDP to have its own checksum. Therefore, IPv6 routers do not need to recompute a checksum when header fields (such as the time to live (TTL) or hop count) change. This improvement may have been made less necessary by the development of routers that perform checksum computation at link speed using dedicated hardware, but it is still relevant for software-based routers.
- The *TTL* field of IPv4 has been renamed to *Hop Limit*, reflecting the fact that routers are no longer expected to compute the time a packet has spent in a queue.

## Mobility

Unlike mobile IPv4, mobile IPv6 avoids triangular routing and is therefore as efficient as native IPv6. IPv6 routers may also allow entire subnets to move to a new router connection point without renumbering.<sup>[31]</sup>

## Options extensibility

The IPv6 protocol header has a fixed size (40 octets). Options are implemented as additional extension headers after the IPv6 header, which limits their size only by the size of an entire packet. The extension header mechanism makes the protocol extensible in that it allows future services for quality of service, security, mobility, and others to be added without redesign of the basic protocol.<sup>[4]</sup>

## Jumbograms

IPv4 limits packets to  $65535 (2^{16}-1)$  octets of payload. An IPv6 node can optionally handle packets over this limit, referred to as jumbograms, which can be as large as  $4294967295 (2^{32}-1)$  octets. The use of jumbograms may improve performance over high-MTU links. The use of jumbograms is indicated by the Jumbo Payload Option header.<sup>[32]</sup>

## Privacy

Like IPv4, IPv6 supports globally unique static IP addresses, which can be used to track a single device's Internet activity. Most devices are used by a single user, so a device's activity is often assumed to be equivalent to a user's activity. This causes privacy concerns in the same way that cookies can also track a user's navigation through sites.

The privacy enhancements in IPv6 have been mostly developed in response to a misunderstanding.<sup>[33]</sup> Interfaces can have addresses based on the MAC address of the machine (the EUI-64 format), but this is not a requirement. Even

when an address is not based on the MAC address though, the interface's address is (contrary to IPv4) usually global instead of local, which makes it much easier to identify a single user through the IP address.

Privacy extensions for IPv6 have been defined to address these privacy concerns.<sup>[34]</sup> When privacy extensions are enabled, the operating system generates ephemeral IP addresses by concatenating a randomly generated host identifier with the assigned network prefix. These ephemeral addresses, instead of trackable static IP addresses, are used to communicate with remote hosts. The use of ephemeral addresses makes it difficult to accurately track a user's Internet activity by scanning activity streams for a single IPv6 address.<sup>[35]</sup>

Privacy extensions are enabled by default in Windows, Mac OS X (since 10.7), and iOS (since version 4.3).<sup>[36]</sup> Some Linux distributions have enabled privacy extensions as well.<sup>[37]</sup>

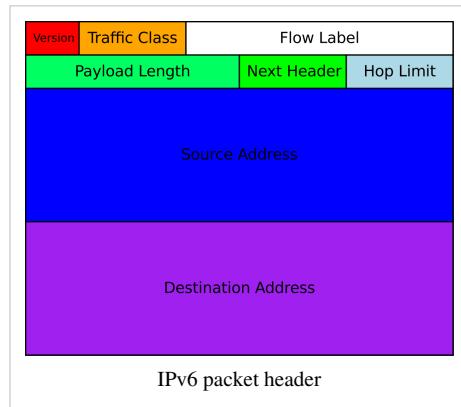
Privacy extensions do not protect the user from other forms of activity tracking, such as tracking cookies. Privacy extensions do little to protect the user from tracking if only one or two hosts are using a given network prefix, and the activity tracker is privy to this information. In this scenario, the network prefix is the unique identifier for tracking. Network prefix tracking is less of a concern if the user's ISP assigns a dynamic network prefix via DHCP.<sup>[38][39]</sup>

## Packet format

An IPv6 packet has two parts: a header and payload.

The header consists of a fixed portion with minimal functionality required for all packets and may be followed by optional extensions to implement special features.

The fixed header occupies the first 40 octets (320 bits) of the IPv6 packet. It contains the source and destination addresses, traffic classification options, a hop counter, and the type of the optional extension or payload which follows the header. This *Next Header* field tells the receiver how to interpret the data which follows the header. If the packet contains options, this field contains the option type of the next option. The "Next Header" field of the last option, points to the upper-layer protocol that is carried in the packet's payload.



Extension headers carry options that are used for special treatment of a packet in the network, e.g., for routing, fragmentation, and for security using the IPsec framework.

Without special options, a payload must be less than 64kB. With a Jumbo Payload option (in a *Hop-By-Hop Options* extension header), the payload must be less than 4 GB.

Unlike in IPv4, routers never fragment a packet. Hosts are expected to use Path MTU Discovery to make their packets small enough to reach the destination without needing to be fragmented. See IPv6 Packet#Fragmentation.

## Addressing

Compared to IPv4, the most obvious advantage of IPv6 is its larger address space. IPv4 addresses are 32 bits long and number about  $4.3 \times 10^9$  (4.3 billion).<sup>[40]</sup> IPv6 addresses are 128 bits long and number about  $3.4 \times 10^{38}$  (340 Undecillion). IPv6's addresses are deemed enough for the foreseeable future.<sup>[41]</sup>

IPv6 addresses are written in eight groups of four hexadecimal digits separated by colons, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IPv6 unicast addresses other than those that start with binary 000 are logically divided into two parts: a 64-bit (sub-)network prefix, and a 64-bit interface identifier.<sup>[42]</sup>

For stateless address autoconfiguration (SLAAC) to work, subnets require a /64 address block, as defined in RFC 4291 section 2.5.1. Local Internet registries get assigned at least /32 blocks, which they divide among ISPs.<sup>[43]</sup> The

obsolete RFC 3177 recommended the assignment of a /48 to end-consumer sites. This was replaced by RFC 6177, which "recommends giving home sites significantly more than a single /64, but does not recommend that every home site be given a /48 either". /56s are specifically considered. It remains to be seen if ISPs will honor this recommendation; for example, during initial trials, Comcast customers were given a single /64 network.<sup>[44]</sup>

IPv6 addresses are classified by three types of networking methodologies: unicast addresses identify each network interface, anycast addresses identify a group of interfaces, usually at different locations of which the nearest one is automatically selected, and multicast addresses are used to deliver one packet to many interfaces. The broadcast method is not implemented in IPv6. Each IPv6 address has a scope, which specifies in which part of the network it is valid and unique. Some addresses are unique only on the local (sub-)network. Others are globally unique.

Some IPv6 addresses are reserved for special purposes, such as loopback, 6to4 tunneling, and Teredo tunneling. See RFC 5156. Also, some address ranges are considered special, such as link-local addresses for use on the local link only, Unique Local addresses (ULA) as described in RFC 4193, and solicited-node multicast addresses used in the Neighbor Discovery Protocol.

## IPv6 in the Domain Name System

In the Domain Name System, hostnames are mapped to IPv6 addresses by AAAA resource records, so-called *quad-A* records. For reverse resolution, the IETF reserved the domain `ip6.arpa`, where the name space is hierarchically divided by the 1-digit hexadecimal representation of nibble units (4 bits) of the IPv6 address. This scheme is defined in RFC 3596.

## Address format

An IPv6 address is represented by 8 groups of 16-bit values, each represented as 4 hexadecimal digits and separated by colons (:). For example:

`2001:0db8:0000:0000:0000:ff00:0042:8329`

The hexadecimal digits are not case-sensitive; e.g., the groups `0DB8` and `0db8` are equivalent.

An IPv6 address may be abbreviated by using one or more of the following rules:

1. Remove leading zeroes from one or more groups of hexadecimal digits; this is normally done to all groups that have leading zeroes. (For example, convert the group `0042` to `42`.)
2. Combine consecutive sections of one or more zeroes, using a double colon (::) to denote the omitted sections. The double colon may only be used once in any given address, as the address would be indeterminate if it was used multiple times. (For example, `2001:db8::1:2` is valid, but `2001:db8::1::2` is not permitted.)

Below is an example of these rules:

Address	2001	:	0db8	:	0000	:	0000	:	0000	:	ff00	:	0042	:	8329
After Rule 1, with leading zeroes removed	2001	:	db8	:	0	:	0	:	0	:	ff00	:	42	:	8329
After Rule 2, with consecutive sections of zeroes combined	2001	:	db8	:						:	ff00	:	42	:	8329

Below are the text representations of these addresses:

Initial address: `2001:0db8:0000:0000:0000:ff00:0042:8329`

After removing leading zeroes: `2001:db8:0:0:0:ff00:42:8329`

After combining consecutive sections of zeroes: `2001:db8::ff00:42:8329`

Another example is the loopback address, which can be abbreviated to `::1` by using both rules above:<sup>[40]</sup>

Initial address: `0000:0000:0000:0000:0000:0000:0000:0001`

After removing leading zeroes: `0:0:0:0:0:0:0:1`

After combining consecutive sections of zeroes: `::1`

As IPv6 addresses may have more than one representation, which can lead to confusion, there is a proposed standard for representing them in text.<sup>[45]</sup>

## Transition mechanisms

Until IPv6 completely supplants IPv4, a number of transition mechanisms<sup>[46]</sup> are needed to enable IPv6-only hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach each-other over IPv4-only infrastructure.

Many of these transition mechanisms use tunneling to encapsulate IPv6 traffic within IPv4 networks. This is an imperfect solution, which may increase latency and cause problems with Path MTU Discovery<sup>[47]</sup>. Tunneling protocols are a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

## Dual IP stack implementation

Dual-stack (or "native dual-stack") refers to side-by-side implementation of IPv4 and IPv6. That is, both protocols run on the same network infrastructure, and there's no need to encapsulate IPv6 inside IPv4 (using tunneling) or vice-versa. Dual-stack is defined in RFC 4213<sup>[48]</sup>.

Although this is the most desired IPv6 implementation, as it avoids the complexities and pitfalls of tunneling, it is not always possible, since outdated network equipment may not support IPv6. A good example is cable TV-based internet access. In modern cable TV networks, the core of the HFC network (such as large core routers) are likely to support IPv6. However, other network equipment (such as a CMTS) or customer equipment (like cable modems) may require software updates or hardware upgrades to support IPv6. This means cable network operators must resort to tunneling until the backbone equipment supports native dual-stack.

## Tunneling

Because not all networks support dual-stack, tunneling is used for IPv4 networks to talk to IPv6 networks (and vice-versa). Many current internet users do not have IPv6 dual-stack support, and thus cannot reach IPv6 sites directly. Instead, they must use IPv4 infrastructure to carry IPv6 packets. This is done using a technique known as *tunneling*, which encapsulates IPv6 packets within IPv4, in effect using IPv4 as a link layer for IPv6.

IP protocol 41 indicates IPv4 packets which encapsulate IPv6 datagrams. Some routers or network address translation devices may block protocol 41. To pass through these devices, you might use UDP packets to encapsulate IPv6 datagrams. Other encapsulation schemes, such as AYIYA or Generic Routing Encapsulation, are also popular.

Conversely, on IPv6-only internet links, when access to IPv4 network facilities is needed, tunneling of IPv4 over IPv6 protocol occurs, using the IPv6 as a link layer for IPv4.

### Automatic tunneling

*Automatic tunneling* refers to a technique where the routing infrastructure automatically determines the tunnel endpoints. Some automatic tunneling techniques are below.

6to4 is recommended by RFC 3056. It uses protocol 41 encapsulation.<sup>[49]</sup> Tunnel endpoints are determined by using a well-known IPv4 anycast address on the remote side, and embedding IPv4 address information within IPv6 addresses on the local side. 6to4 is the most common tunnel protocol currently deployed.

*Teredo* is an automatic tunneling technique that uses UDP encapsulation and can allegedly cross multiple NAT boxes.<sup>[50]</sup> IPv6, including 6to4 and Teredo tunneling, are enabled by default in Windows Vista<sup>[51]</sup> and Windows 7. Most Unix systems implement only 6to4, but Teredo can be provided by third-party software such as Miredo.

*ISATAP*<sup>[52]</sup> treats the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link-local IPv6 address. Unlike 6to4 and Teredo, which are *inter-site* tunnelling mechanisms, ISATAP is an *intra-site*

mechanism, meaning that it is designed to provide IPv6 connectivity between nodes within a single organisation.

### Configured and automated tunneling (6in4)

In *configured tunneling*, the tunnel endpoints are explicitly configured, either by an administrator manually or the operating system's configuration mechanisms, or by an automatic service known as a tunnel broker,<sup>[53]</sup> this is also referred to as *automated tunneling*. Configured tunneling is usually more deterministic and easier to debug than automatic tunneling, and is therefore recommended for large, well-administered networks. Automated tunneling provides a compromise between the ease of use of automatic tunneling and the deterministic behaviour of configured tunneling.

Raw encapsulation of IPv6 packets using IPv4 protocol number 41 is recommended for configured tunneling; this is sometimes known as 6in4 tunneling. As with automatic tunneling, encapsulation within UDP may be used in order to cross NAT boxes and firewalls.

### Proxying and translation for IPv6-only hosts

After the regional Internet registries have exhausted their pools of available IPv4 addresses, it is likely that hosts newly added to the Internet might only have IPv6 connectivity. For these clients to have backward-compatible connectivity to existing IPv4-only resources, suitable IPv6 transition mechanisms must be deployed.

One form of address translation is the use of a dual-stack application-layer proxy server, for example a web proxy.

NAT-like techniques for application-agnostic translation at the lower layers in routers and gateways have been proposed. The NAT-PT standard was dropped due to a number of criticisms,<sup>[54]</sup> however more recently the continued low adoption of IPv6 has prompted a new standardization effort under the name NAT64.

## IPv6 readiness

Compatibility with IPv6 networking is mainly a software or firmware issue. However, much of the older hardware that could in principle be upgraded is likely to be replaced instead. The American Registry for Internet Numbers (ARIN) suggested that all Internet servers be prepared to serve IPv6-only clients by January 2012.<sup>[55]</sup> Sites will only be accessible over NAT64 if they do not use IPv4 literals as well.

## Software

Applications can be IPv4 only, IPv6 only, dual-stack, or hybrid dual-stack. Most personal computers running recent operating system versions are IPv6-ready. Many popular applications with network capabilities are ready, and most others could be easily upgraded with help from the developers.

Some software transitioning mechanisms are outlined in RFC 4038, RFC 3493, and RFC 3542.

### IPv4-mapped IPv6 addresses

Hybrid dual-stack IPv6/IPv4 implementations recognize a special class of addresses, the IPv4-mapped IPv6 addresses. In these addresses, the first 80 bits are zero, the next 16 bits are one, and the remaining 32 bits are the IPv4 address. You may see these addresses with the first 96 bits written in the standard IPv6 format, and the remaining 32 bits written in the customary dot-decimal notation of IPv4. For example, `:ffff:192.0.2.128` represents the IPv4 address `192.0.2.128`. A deprecated format for IPv4-compatible IPv6 addresses was `::192.0.2.128`.<sup>[56]</sup>

Because of the significant internal differences between IPv4 and IPv6, some of the lower-level functionality available to programmers in the IPv6 stack does not work identically with IPv4-mapped addresses. Some common IPv6 stacks do not implement the IPv4-mapped address feature, either because the IPv6 and IPv4 stacks are separate implementations (e.g., Microsoft Windows 2000, XP, and Server 2003), or because of security concerns

(OpenBSD).<sup>[57]</sup> On these operating systems, a program must open a separate socket for each IP protocol it uses. On some systems, e.g., the Linux kernel, NetBSD, and FreeBSD, this feature is controlled by the socket option `IPV6_V6ONLY`, as specified in RFC 3493.<sup>[58]</sup>

## Hardware and embedded systems

Low-level equipment such as network adapters and network switches may not be affected by the change, since they transmit link-layer frames without inspecting the contents. However, networking devices that obtain IP addresses or perform routing of IP packets do need to understand IPv6.

Most equipment would be IPv6 capable with a software or firmware update if the device has sufficient storage and memory space for the new IPv6 stack. However, manufacturers may be reluctant to spend on software development costs for hardware they have already sold when they are poised for new sales from IPv6-ready equipment.

In some cases, non-compliant equipment needs to be replaced because the manufacturer no longer exists or software updates are not possible, for example, because the network stack is implemented in permanent read-only memory.

The CableLabs consortium published the 160 Mbit/s DOCSIS 3.0 IPv6-ready specification for cable modems in August 2006. The widely used DOCSIS 2.0 does not support IPv6. The new 'DOCSIS 2.0 + IPv6' standard supports IPv6, which may on the cable modem side require only a firmware upgrade.<sup>[59][60]</sup> It is expected that only 60% of cable modems' servers and 40% of cable modems will be DOCSIS 3.0 by 2011.<sup>[61]</sup> However, most ISPs that support DOCSIS 3.0 do not support IPv6 across their networks.

Other equipment which is typically not IPv6-ready ranges from Voice over Internet Protocol devices to laboratory equipment and printers.

## Deployment

The introduction of Classless Inter-Domain Routing (CIDR) in the Internet routing and IP address allocation methods in 1993 and the extensive use of network address translation (NAT) delayed the inevitable IPv4 address exhaustion, but the final phase of exhaustion started on February 3, 2011.<sup>[17]</sup> However, despite a decade long development and implementation history as a Standards Track protocol, general worldwide deployment is still in its infancy. As of October 2011, about 3% of domain names and 12% of the networks on the internet have IPv6 protocol support.<sup>[62]</sup>

IPv6 has been implemented on all major operating systems in use in commercial, business, and home consumer environments. Since 2008, the domain name system can be used in IPv6. IPv6 was first used in a major world event during the 2008 Summer Olympic Games,<sup>[63]</sup> the largest showcase of IPv6 technology since the inception of IPv6.<sup>[64]</sup> Countries like China and the Federal U.S. Government are also starting to require IPv6 capability on their equipment.

In 2010, Verizon mandated IPv6 operation and deprecated IPv4 as an optional capability for cellular hardware.<sup>[65]</sup> T-Mobile USA followed suit. As of June 2012, T-Mobile supports external IPv6 access.<sup>[66]</sup>

## References

- [1] David Frost (2011-04-20). "Ipv6 traffic volumes going backwards" (<http://www.itwire.com/business-it-news/networking/46689-ipv6-traffic-volumes-going-backwards>). iTWire. . Retrieved 2012-02-19.
- [2] Goldman, David. "The Internet now has 340 trillion trillion addresses" (<http://money.cnn.com/2012/06/06/technology/ipv6/index.htm>). CNN. . Retrieved 2012-06-23.
- [3] Graph of IPv6 share from May 15th to June 14th, 2012 (<http://ddos.arbornetworks.com/uploads/2012/06/IJ13.jpg>) at arbornetworks.com
- [4] RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, S. Deering, R. Hinden (December 1998)
- [5] Google IPv6 Conference 2008: What will the IPv6 Internet look like? (<http://www.youtube.com/watch?v=mZo69JQoLb8>). Event occurs at 13:35. .
- [6] RFC 1752 *The Recommendation for the IP Next Generation Protocol*, S. Bradner, A. Mankin, January 1995.
- [7] Rashid, Fahmida. "IPv4 Address Exhaustion Not Instant Cause for Concern with IPv6 in Wings" (<http://www.eweek.com/c/a/IT-Infrastructure/IPv4-Address-Exhaustion-Not-Instant-Cause-for-Concern-with-IPv6-in-Wings-287643/>). eWeek. . Retrieved 2012-06-23.
- [8] RFC 1550, *IP: Next Generation (IPng) White Paper Solicitation*, S. Bradner, A. Mankin (December 1993)
- [9] "History of the IPng Effort" (<http://playground.sun.com/ipv6/doc/history.html>). Sun. .
- [10] "River of IPv4 addresses officially runs dry" (<http://arstechnica.com/tech-policy/news/2011/02/river-of-ipv4-addresses-officially-runs-dry>). arstechnica.com. .
- [11] Rashid, Fahmida Y. (February 3, 2011). "IPv4 Address Depletion Adds Momentum to IPv6 Transition" (<http://www.eweek.com/c/a/IT-Infrastructure/IPv4-Address-Depletion-Adds-Momentum-to-IPv6-Transition-875751/>). eWeek.com. . Retrieved February 3, 2011.
- [12] "Two /8s allocated to APNIC from IANA" (<http://www.apnic.net/publications/news/2011/delegation>). APNIC. 2010-01-01. . Retrieved 2011-02-03.
- [13] Asia-Pacific Network Information Centre (15 April 2011). "APNIC IPv4 Address Pool Reaches Final /8" (<http://www.apnic.net/publications/news/2011/final-8>). . Retrieved 15 April 2011.
- [14] Exec: No shortage of Net addresses By John Lui, CNETAsia ([http://news.zdnet.com/2100-1009\\_22-1020653.html](http://news.zdnet.com/2100-1009_22-1020653.html))
- [15] "A Pragmatic Report on IPv4 Address Space Consumption by Tony Hain, Cisco Systems" ([http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_8-3/ipv4.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html)). Cisco.com. 2005-07-01. . Retrieved 2012-02-19.
- [16] Proposed Global Policy for the Allocation of the Remaining IPv4 Address Space (<http://www.ripe.net/ripe/policies/proposals/2008-03.html>)
- [17] "IPv4 Address Report" (<http://www.potaroo.net/tools/ipv4/>). Potaroo.net. . Retrieved 2012-01-20.
- [18] RFC 1726, *Technical Criteria for Choosing IP The Next Generation (IPng)*, Partridge C., Kastenholz F. (December 1994)
- [19] "U.S. Census Bureau" (<http://www.census.gov/main/www/popclock.html>). Census.gov. . Retrieved 2012-01-20.
- [20] "Moving to IPv6: Now for the hard part (FAQ)" ([http://news.cnet.com/8301-30685\\_3-20030482-264.html](http://news.cnet.com/8301-30685_3-20030482-264.html)). Deep Tech. CNET News. . Retrieved 2011-02-03.
- [21] RFC 2071, *Network Renumbering Overview: Why would I want it and what is it anyway?*, P. Ferguson, H. Berkowitz (January 1997)
- [22] RFC 2072, *Router Renumbering Guide*, H. Berkowitz (January 1997)
- [23] RFC 4862, *IPv6 Stateless Address Autoconfiguration*, S. Thomson, T. Narten, T. Jinmei (September 2007)
- [24] RFC 1112, *Host extensions for IP multicasting*, S. Deering (August 1989)
- [25] RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*, P. Savola, B. Haberman (November 2004)
- [26] RFC 2908, *The Internet Multicast Address Allocation Architecture*, D. Thaler, M. Handley, D. Estrin (September 2000)
- [27] RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*, B. Haberman, D. Thaler (August 2002)
- [28] RFC 2894, *Router Renumbering for IPv6*, M. Crawford, August 2000.
- [29] RFC 4301, *IPv6 Node Requirements*, J. Loughney (April 2006)
- [30] RFC 6434, "IPv6 Node Requirements", E. Jankiewicz, J. Loughney, T. Narten (December 2011)
- [31] RFC 3963, *Network Mobility (NEMO) Basic Protocol Support*, V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert (January 2005)
- [32] RFC 2675, *IPv6 Jumbograms*, D. Borman, S. Deering, R. Hinden (August 1999)
- [33] IPv6 Essentials by Silvia Hagen, p. 28, chapter 3.5.
- [34] T. Narten, R. Draves (2001-01). "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" (<http://www.ietf.org/rfc/rfc3041.txt>). .
- [35] Privacy Extensions (IPv6) (<http://www.elektronik-kompendium.de/sites/net/1601271.htm>), Elektronik Kompendium.
- [36] IPv6: Privacy Extensions einschalten (<http://www.heise.de/netze/artikel/IPv6-Privacy-Extensions-einschalten-1204783.html>), Reiko Kaps, 2011-04-13
- [37] "Comment #61 : Bug #176125 : Bugs: "procps" package: Ubuntu" (<https://bugs.launchpad.net/ubuntu/+source/procps/+bug/176125/comments/61>). Bugs.launchpad.net. . Retrieved 2012-02-19.
- [38] Statement on IPv6 Address Privacy (<ftp://ftp.cuhk.edu.hk/pub/doc/ipng/html/ipv6-address-privacy.html>), Steve Deering & Bob Hinden, Co-Chairs of the IETF's IP Next Generation Working Group, 1999-11-06.
- [39] "Neues Internet-Protokoll erschwert anonymes Surfen" (<http://www.spiegel.de/netzwelt/web/0,1518,729340,00.html>). Spiegel.de. . Retrieved 2012-02-19.
- [40] RFC 4291 *IP Version 6 Addressing Architecture*, R. Hinden, S. Deering (February 2006)
- [41] "The sheer size of IPv6" (<http://pthree.org/2009/03/08/the-sheer-size-of-ipv6/>). Pthre.org. 2009-03-08. . Retrieved 2012-01-20.

- [42] RFC 4291 p. 9
- [43] "IPv6 Address Allocation and Assignment Policy" (<http://www.ripe.net/ripe/docs/ripe-512>). RIPE NCC. 8 February 2011.. Retrieved 27 March 2011.
- [44] "Comcast Activates First Users With IPv6 Native Dual Stack Over DOCSIS" (<http://blog.comcast.com/2011/01/comcast-activates-first-users-with-ipv6-native-dual-stack-over-docsis.html>). Comcast. 31 January 2011..
- [45] RFC 5952, *A Recommendation for IPv6 Address Text Representation*, S. Kawamura (August 2010)
- [46] "IPv6 Transition Mechanism / Tunneling Comparison" (<http://www.sixxs.net/faq/connectivity/?faq=comparison>). Sixxs.net. . Retrieved 2012-01-20.
- [47] "RFC 6343 - Advisory Guidelines for 6to4 Deployment" (<http://tools.ietf.org/html/rfc6343>). Tools.ietf.org. . Retrieved 2012-08-20.
- [48] "RFC 4213 - Basic Transition Mechanisms for IPv6 Hosts and Routers" (<http://tools.ietf.org/html/rfc4213>). Tools.ietf.org. . Retrieved 2012-08-20.
- [49] RFC 3056 *Connection of IPv6 Domains via IPv4 Clouds*, B. Carpenter, Februari 2001.
- [50] RFC 4380 *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*, C. Huitema, Februari 2006
- [51] "The Windows Vista Developer Story: Application Compatibility Cookbook" (<http://msdn2.microsoft.com/en-us/library/aa480152.aspx>). Msdn2.microsoft.com. 2006-04-24.. Retrieved 2012-01-20.
- [52] RFC 5214 *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*, F. Templin, T. Gleeson, D. Thaler, March 2008.
- [53] RFC 3053, *IPv6 Tunnel Broker*, A. Durand, P. Fasano, I. Guardini, D. Lento (January 2001)
- [54] RFC 4966 Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic Status
- [55] *Web sites must support IPv6 by 2012, expert warns* (<http://www.networkworld.com/news/2010/012110-ipv6-warning.html>). Network World. 21 January 2010.. Retrieved 2010-09-30.
- [56] "RFC4291" (<http://tools.ietf.org/html/rfc4291>). Tools.ietf.org. . Retrieved 2012-01-20.
- [57] "OpenBSD inet6(4) manual page" (<http://www.openbsd.org/cgi-bin/man.cgi?query=inet6&apropos=0&sektion=0&manpath=OpenBSD+Current&arch=i386&format=html#PROTOCOLS>). Openbsd.org. 2009-12-13.. Retrieved 2012-01-20.
- [58] "RFC 3493 - Basic Socket Interface Extensions for IPv6" (<http://tools.ietf.org/html/rfc3493#page-22>). Tools.ietf.org. . Retrieved 2012-01-20.
- [59] "DOCSIS 2.0 Interface" (<http://www.cablemodem.com/specifications/specifications20.html>). Cablemodem.com. 2007-10-29.. Retrieved 2009-08-31.
- [60] "RMV6TF.org" ([http://rmv6tf.org/2008-IPv6-Summit-Presentations/Dan\\_Torbet\\_-\\_IPv6andCablev2.pdf](http://rmv6tf.org/2008-IPv6-Summit-Presentations/Dan_Torbet_-_IPv6andCablev2.pdf)) (PDF). . Retrieved 2012-01-20.
- [61] "DOCSIS 3.0 Network Equipment Penetration to Reach 60% by 2011" (<http://www.abiresearch.com/abiprdisplay.jsp?pressid=710>) (Press release). ABI Research. 2007-08-23.. Retrieved 2007-09-30.
- [62] Mike Leber (2010-10-02). "Global IPv6 Deployment Progress Report" (<http://bgp.he.net/ipv6-progress-report.cgi>). Hurricane Electric. . Retrieved 2011-10-19.
- [63] "Beijing2008.cn leaps to next-generation Net" (<http://en.beijing2008.cn/news/official/preparation/n214384681.shtml>) (Press release). The Beijing Organizing Committee for the Games of the XXIX Olympiad. 2008-05-30..
- [64] Das, Kaushik (2008). "IPv6 and the 2008 Beijing Olympics" (<http://ipv6.com/articles/general/IPv6-Olympics-2008.htm>). *IPv6.com*. . Retrieved 2008-08-15. "As thousands of engineers, technologists have worked for a significant time to perfect this (IPv6) technology, there is no doubt, this technology brings considerable promises but this is for the first time that it will showcase its strength when in use for such a mega-event."
- [65] Derek Morr (2009-06-09). "Verizon Mandates IPv6 Support for Next-Gen Cell Phones" ([http://www.circleid.com/posts/20090609\\_verizon\\_mandates\\_ipv6\\_support\\_for\\_next\\_gen\\_cell\\_phones/](http://www.circleid.com/posts/20090609_verizon_mandates_ipv6_support_for_next_gen_cell_phones/)). CircleID. .
- [66] theip6guy (2012-07-31). "T-Mobile USA Launches External IPv6" (<https://support.t-mobile.com/thread/27171>). T-Mobile. .

## External links

- IPv6 (<http://www.dmoz.org/Computers/Internet/Protocols/IP/IPv6/>) at the Open Directory Project
- Why IPv6 matters to radio stations (<http://radioworld.com/article/why-ipv6-matters-to-your-station/23533>)
- Security implications of implementing IPv6 ([https://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert\\_inf\\_security\\_implications\\_ipv6.pdf](https://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_security_implications_ipv6.pdf))
- Free Pool of IPv4 Address Space Depleted (<https://www.nro.net/news/ipv4-free-pool-depleted>)
- An article about IPv6 in Linux by Rami Rosen (<http://www.linuxfordevices.com/c/a/Linux-For-Devices-Articles/IPv6-in-Linux/>)
- An Introduction and Statistics about IPV6 (<https://www.google.com/intl/en/ipv6/>)
- test-ipv6.com/ (<https://test-ipv6.com/>), checks your connection.
- Google IPv6 check (<https://ipv6test.google.com/>)
- IPv6 Introduction and Configuration (<https://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/redp4776.html?OpenDocument>) by IBM Redbooks

# Dynamic Host Configuration Protocol

The **Dynamic Host Configuration Protocol (DHCP)** is a network protocol that is used to configure network devices so that they can communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route and one or more DNS server addresses from a DHCP server. The DHCP client then uses this information to configure its host. Once the configuration process is complete, the host is able to communicate on the internet.

The DHCP server maintains a database of available IP addresses and configuration information. When it receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, and then allocates an IP address or prefix that is appropriate for the client, and sends configuration information appropriate for that client.

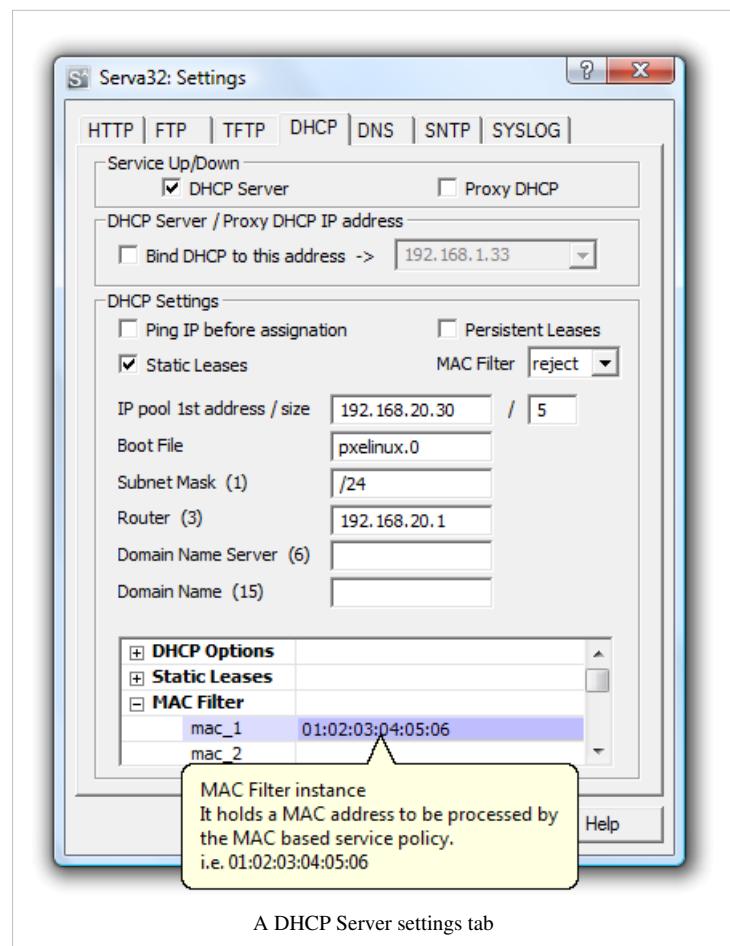
Because the DHCP protocol must work correctly even before DHCP clients have been configured, the DHCP server and DHCP client

must be connected to the same network link. In larger networks, this is not practical. On such networks, each network link contains one or more DHCP relay agents. These DHCP relay agents receive messages from DHCP clients and forward them to DHCP servers. DHCP servers send responses back to the relay agent, and the relay agent then sends these responses to the DHCP client on the local network link.

DHCP servers typically grant IP addresses to clients only for a limited interval. DHCP clients are responsible for renewing their IP address before that interval has expired, and must stop using the address once the interval has expired, if they have not been able to renew it.

DHCP is used for IPv4 and IPv6. While both versions serve much the same purpose, the details of the protocol for IPv4 and IPv6 are sufficiently different that they may be considered separate protocols.<sup>[1]</sup>

Hosts that do not use DHCP for address configuration may still use it to obtain other configuration information. Alternatively, IPv6 hosts may use stateless address autoconfiguration. IPv4 hosts may use link-local addressing to achieve limited local connectivity.



A DHCP Server settings tab

## History

DHCP was first defined as a standards track protocol in RFC 1531 in October 1993, as an extension to the Bootstrap Protocol (BOOTP). The motivation for extending BOOTP was that BOOTP required manual intervention to add configuration information for each client, and did not provide a mechanism for reclaiming disused IP addresses.

Many worked to clarify the protocol as it gained popularity, and in 1997 RFC 2131 was released, and remains as of 2011 the standard for IPv4 networks. DHCPv6 is documented in RFC 3315. RFC 3633 added a DHCPv6 mechanism for prefix delegation. DHCPv6 was further extended to provide configuration information to clients configured using stateless address autoconfiguration in RFC 3736.

The BOOTP protocol itself was first defined in RFC 951 as a replacement for the Reverse Address Resolution Protocol RARP. The primary motivation for replacing RARP with BOOTP was that RARP was a data link layer protocol. This made implementation difficult on many server platforms, and required that a server be present on each individual network link. BOOTP introduced the innovation of a *relay agent*, which allowed the forwarding of BOOTP packets off the local network using standard IP routing, thus one central BOOTP server could serve hosts on many IP subnets.<sup>[2]</sup>

## Technical overview

Dynamic Host Configuration Protocol automates network-parameter assignment to network devices from one or more DHCP servers. Even in small networks, DHCP is useful because it makes it easy to add new machines to the network.

When a DHCP-configured client (a computer or any other network-aware device) connects to a network, the DHCP client sends a broadcast query requesting necessary information to a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, other servers such as time servers, and so forth. On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting, and must complete before the client can initiate IP-based communication with other hosts. Upon disconnecting, the IP address is returned to the pool for use by another computer. This way, many other computers can use the same IP address within minutes of each other.

Depending on implementation, the DHCP server may have three methods of allocating IP-addresses:

- *dynamic allocation*: A network administrator assigns a range of IP addresses to DHCP, and each client computer on the LAN is configured to request an IP address from the DHCP server during network initialization. The request-and-grant process uses a lease concept with a controllable time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed.
- *automatic allocation*: The DHCP server permanently assigns a free IP address to a requesting client from the range defined by the administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.
- *static allocation*: The DHCP server allocates an IP address based on a table with MAC address/IP address pairs, which are manually filled in (perhaps by a network administrator). [Only requesting clients with a MAC address listed in this table will be allocated an IP address]. This feature (which is not supported by all DHCP servers) is variously called *Static DHCP Asignment* (by DD-WRT), *fixed-address* (by the dhcpcd documentation), *Address Reservation* (by Netgear), *DHCP reservation* or *Static DHCP* (by Cisco/Linksys), and *IP reservation* or *MAC/IP binding* (by various other router manufacturers).

## Technical details

DHCP uses the same two ports assigned by IANA for BOOTP: destination UDP port 67 for sending data to the server, and UDP port 68 for data to the client. DHCP communications are connectionless in nature.

DHCP operations fall into four basic phases: IP discovery, IP lease offer, IP request, and IP lease acknowledgement. These points are often abbreviated as DORA (Discovery, Offer, Request, Acknowledgement).

DHCP clients and servers on the same subnet communicate via UDP broadcasts, initially. If the client and server are on different subnets, a DHCP Helper or DHCP Relay Agent may be used. Clients requesting renewal of an existing lease may communicate directly via UDP unicast, since the client already has an established IP address at that point.

### DHCP discovery

The client broadcasts messages on the physical subnet to discover available DHCP servers. Network administrators can configure a local router to forward DHCP packets to a DHCP server from a different subnet. This client-implementation creates a User Datagram Protocol (UDP) packet with the broadcast destination of 255.255.255.255 or the specific subnet broadcast address.

A DHCP client can also request its last-known IP address (in the example below, 192.168.1.100). If the client remains connected to a network for which this IP is valid, the server may grant the request. Otherwise, it depends whether the server is set up as authoritative or not. An authoritative server will deny the request, making the client ask for a new IP address immediately. A non-authoritative server simply ignores the request, leading to an implementation-dependent timeout for the client to give up on the request and ask for a new IP address.

### DHCPDISCOVER

UDP Src=0.0.0.0 sPort=68 Dest=255.255.255 dPort=67					
<b>OP</b>	<b>HTYPE</b>	<b>HLEN</b>	<b>HOPS</b>		
0x01	0x01	0x06	0x00		
<b>XID</b>					
0x3903F326					
<b>SECS</b>		<b>FLAGS</b>			
0x0000		0x0000			
<b>CIADDR (Client IP Address)</b>					
0x00000000					
<b>YIADDR (Your IP Address)</b>					
0x00000000					
<b>SIADDR (Server IP Address)</b>					
0x00000000					
<b>GIADDR (Gateway IP Address)</b>					
0x00000000					
<b>CHADDR (Client Hardware Address)</b>					
0x00053C04					
0x8D590000					
0x00000000					
0x00000000					

192 octets of 0s, or overflow space for additional options. BOOTP legacy
<b>Magic Cookie</b>
0x63825363
<b>DHCP Options</b>
DHCP option 53: DHCP Discover
DHCP option 50: 192.168.1.100 requested
DHCP option 55: Parameter Request List: Request Subnet Mask (1), Router (3), Domain Name (15), Domain Name Server (6)

## DHCP offer

When a DHCP server receives an IP lease request from a client, it reserves an IP address for the client and extends an IP lease offer by sending a DHCPOFFER message to the client. This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer.

The server determines the configuration based on the client's hardware address as specified in the CHADDR (Client Hardware Address) field. Here the server, 192.168.1.1, specifies the IP address in the YIADDR (Your IP Address) field.

## DHCPOFFER

UDP Src=192.168.1.1 sPort=67 Dest=255.255.255.255 dPort=68			
<b>OP</b>	<b>HTYPE</b>	<b>HLEN</b>	<b>HOPS</b>
0x02	0x01	0x06	0x00
0x00000000			
<b>YIADDR (Your IP Address)</b>			
0xC0A80164			
<b>SIADDR (Server IP Address)</b>			
0xC0A80101			
<b>GIADDR (Gateway IP Address)</b>			
0x00000000			
<b>CHADDR (Client Hardware Address)</b>			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s. BOOTP legacy			
<b>Magic Cookie</b>			
0x63825363			
<b>DHCP Options</b>			
DHCP option 53: DHCP Offer			
DHCP option 1: 255.255.255.0 subnet mask			

DHCP option 3: 192.168.1.1 router
DHCP option 51: 86400s (1 day) IP lease time
DHCP option 54: 192.168.1.1 DHCP server
DHCP option 6: DNS servers 9.7.10.15, 9.7.10.16, 9.7.10.18

## DHCP request

In response to the offer Client requests the server. The client replies DHCPRequest, unicast to the server, requesting the offered address. A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer. Based on the Transaction ID field in the request, servers are informed whose offer the client has accepted. When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses. In some cases DHCP request message is broadcast, instead of being unicast to a particular DHCP server, because the DHCP client has still not received an IP address. Also, this way one message can let all other DHCP servers know that another server will be supplying the IP address without missing any of the servers with a series of unicast messages.

### DHCPREQUEST

UDP Src=0.0.0.0 sPort=68 Dest=255.255.255.255 dPort=67					
<b>OP</b>	<b>HTYPE</b>	<b>HLEN</b>	<b>HOPS</b>		
0x01	0x01	0x06	0x00		
<b>XID</b>					
0x3903F326					
<b>SECS</b>		<b>FLAGS</b>			
0x0000		0x0000			
<b>CIADDR (Client IP Address)</b>					
0x00000000					
<b>YIADDR (Your IP Address)</b>					
0x00000000					
<b>SIADDR (Server IP Address)</b>					
0xC0A80101					
<b>GIADDR (Gateway IP Address)</b>					
0x00000000					
<b>CHADDR (Client Hardware Address)</b>					
0x00053C04					
0x8D590000					
0x00000000					
0x00000000					
192 octets of 0s. BOOTP legacy					
<b>Magic Cookie</b>					
0x63825363					
<b>DHCP Options</b>					

DHCP option 53: DHCP Request
DHCP option 50: 192.168.1.100 requested
DHCP option 54: 192.168.1.1 DHCP server.

## DHCP acknowledgement

When the DHCP server receives the DHCPREQUEST message from the client, the configuration process enters its final phase. The acknowledgement phase involves sending a DHCPACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested. At this point, the IP configuration process is completed.

The protocol expects the DHCP client to configure its network interface with the negotiated parameters.

## DHCPACK

UDP Src=192.168.1.1 sPort=67 Dest=255.255.255 dPort=68					
<b>OP</b>	<b>HTYPE</b>	<b>HLEN</b>	<b>HOPS</b>		
0x02	0x01	0x06	0x00		
<b>XID</b>					
0x3903F326					
<b>SECS</b>		<b>FLAGS</b>			
0x0000	0x0000				
<b>CIADDR (Client IP Address)</b>					
0x00000000					
<b>YIADDR (Your IP Address)</b>					
0xC0A80164					
<b>SIADDR (Server IP Address)</b>					
0xC0A80101					
<b>GIADDR (Gateway IP Address switched by relay)</b>					
0x00000000					
<b>CHADDR (Client Hardware Address)</b>					
0x00053C04					
0x8D590000					
0x00000000					
0x00000000					
192 octets of 0s. BOOTP legacy					
<b>Magic Cookie</b>					
0x63825363					
<b>DHCP Options</b>					
DHCP option 53: DHCP ACK					
DHCP option 1: 255.255.255.0 subnet mask					
DHCP option 3: 192.168.1.1 router					

DHCP option 51: 86400s (1 day) IP lease time	
DHCP option 54: 192.168.1.1 DHCP server	
DHCP option 6: DNS servers 9.7.10.15, 9.7.10.16, 9.7.10.18	

After the client obtains an IP address, the client may use the Address Resolution Protocol (ARP) to prevent IP conflicts caused by overlapping address pools of DHCP servers.

## DHCP information

A DHCP client may request more information than the server sent with the original DHCPOFFER. The client may also request repeat data for a particular application. For example, browsers use *DHCP Inform* to obtain web proxy settings via WPAD. Such queries do not cause the DHCP server to refresh the IP expiry time in its database.

## DHCP releasing

The client sends a request to the DHCP server to release the DHCP information and the client deactivates its IP address. As client devices usually do not know when users may unplug them from the network, the protocol does not mandate the sending of *DHCP Release*.

## Client configuration parameters in DHCP

A DHCP server can provide optional configuration parameters to the client. RFC 2132 describes the available DHCP options defined by Internet Assigned Numbers Authority (IANA) - DHCP and BOOTP PARAMETERS <sup>[3]</sup>.

A DHCP client can select, manipulate and overwrite parameters provided by a DHCP server.<sup>[4]</sup>

## DHCP options

The following tables list the available DHCP options, as stated in RFC2132.<sup>[5]</sup>

### RFC1497 vendor extensions<sup>[6]</sup>

Code	Name	Length	Notes
0	Pad <sup>[7]</sup>	1 octet	Can be used to pad other options so that they are aligned to the word boundary
1	Subnet Mask <sup>[8]</sup>	4 octets	Must be sent after the router option (option 3) if both are included
2	Time Offset <sup>[9]</sup>	4 octets	
3	Router	multiples of 4 octets	Available routers, should be listed in order of preference
4	Time Server	multiples of 4 octets	Available time servers to synchronise with, should be listed in order of preference
5	Name Server	multiples of 4 octets	Available IEN116 name servers, should be listed in order of preference
6	Domain Name Server	multiples of 4 octets	Available DNS servers, should be listed in order of preference
7	Log Server	multiples of 4 octets	Available log servers, should be listed in order of preference.
8	Cookie Server	multiples of 4 octets	
9	LPR Server	multiples of 4 octets	
10	Impress Server	multiples of 4 octets	
11	Resource Location Server	multiples of 4 octets	
12	Host Name	minimum of 1 octet	
13	Boot File Size	2 octets	Length of the boot image in 4KiB blocks

14	Merit Dump File	minimum of 1 octet	Path where crash dumps should be stored
15	Domain Name	minimum of 1 octet	
16	Swap Server	4 octets	
17	Root Path	minimum of 1 octet	
18	Extensions Path	minimum of 1 octet	
255	End	1 octet	Used to mark the end of the vendor option field

### IP Layer Parameters per Host<sup>[10]</sup>

Code	Name	Length	Notes
19	IP Forwarding Enable/Disable	1 octet	
20	Non-Local Source Routing Enable/Disable	1 octet	
21	Policy Filter	multiples of 8 octets	
22	Maximum Datagram Reassembly Size	2 octets	
23	Default IP Time-to-live	1 octet	
24	Path MTU Aging Timeout	4 octets	
25	Path MTU Plateau Table	multiples of 2 octets	

### IP Layer Parameters per Interface<sup>[11]</sup>

Code	Name	Length	Notes
26	Interface MTU	2 octets	
27	All Subnets are Local	1 octet	
28	Broadcast Address	4 octets	
29	Perform Mask Discovery	1 octet	
30	Mask Supplier	1 octet	
31	Perform Router Discovery	1 octet	
32	Router Solicitation Address	4 octets	
33	Static Route	multiples of 8 octets	A list of destination/router pairs

### Link Layer Parameters per Interface<sup>[12]</sup>

Code	Name	Length	Notes
34	Trailer Encapsulation Option	1 octet	
35	ARP Cache Timeout	4 octets	
36	Ethernet Encapsulation	1 octet	

**TCP Parameters<sup>[13]</sup>**

<b>Code</b>	<b>Name</b>	<b>Length</b>	<b>Notes</b>
37	TCP Default TTL	1 octet	
38	TCP Keepalive Interval	4 octets	
39	TCP Keepalive Garbage	1 octet	

**Application and Service Parameters<sup>[14]</sup>**

<b>Code</b>	<b>Name</b>	<b>Length</b>	<b>Notes</b>
40	Network Information Service Domain	minimum of 1 octet	
41	Network Information Servers	multiples of 4 octets	
42	Network Time Protocol Servers	multiples of 4 octets	
43	Vendor Specific Information	minimum of 1 octets	
44	NetBIOS over TCP/IP Name Server	multiples of 4 octets	
45	NetBIOS over TCP/IP Datagram Distribution Server	multiples of 4 octets	
46	NetBIOS over TCP/IP Node Type	1 octet	
47	NetBIOS over TCP/IP Scope	minimum of 1 octet	
48	X Window System Font Server	multiples of 4 octets	
49	X Window System Display Manager	multiples of 4 octets	
64	Network Information Service+ Domain	minimum of 1 octet	
65	Network Information Service+ Servers	multiples of 4 octets	
68	Mobile IP Home Agent	multiples of 4 octets	
69	Simple Mail Transport Protocol (SMTP) Server	multiples of 4 octets	
70	Post Office Protocol (POP3) Server	multiples of 4 octets	
71	Network News Transport Protocol (NNTP) Server	multiples of 4 octets	
72	Default World Wide Web (WWW) Server	multiples of 4 octets	
73	Default Finger Server	multiples of 4 octets	
74	Default Internet Relay Chat (IRC) Server	multiples of 4 octets	
75	StreetTalk Server	multiples of 4 octets	
76	StreetTalk Directory Assistance (STDA) Server	multiples of 4 octets	

## DHCP Extensions<sup>[15]</sup>

Code	Name	Length	Notes
50	Requested IP Address	4 octets	
51	IP Address Lease Time	4 octets	
52	Option Overload	1 octet	
66	TFTP server name	minimum of 1 octet	
67	Bootfile name	minimum of 1 octet	
53	DHCP Message Type	1 octet	
54	Server Identifier	4 octets	
55	Parameter Request List	minimum of 1 octet	
56	Message	minimum of 1 octet	
57	Maximum DHCP Message Size	2 octets	
58	Renewal (T1) Time Value	4 octets	
59	Rebinding (T2) Time Value	4 octets	
60	Vendor class identifier	minimum of 1 octet	
61	Client-identifier	minimum of 2 octets	

### Vendor identification

An option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters or octets which has a meaning specified by the vendor of the DHCP client. One method that a DHCP client can utilize to communicate to the server that it is using a certain type of hardware or firmware is to set a value in its DHCP requests called the Vendor Class Identifier (VCI) (Option 60). This method allows a DHCP server to differentiate between the two kinds of client machines and process the requests from the two types of modems appropriately. Some types of set-top boxes also set the VCI (Option 60) to inform the DHCP server about the hardware type and functionality of the device. The value that this option is set to give the DHCP server a hint about any required extra information that this client needs in a DHCP response.

### DHCP relaying

In small networks, where only one IP subnet is being managed, DHCP clients communicate directly with DHCP servers. However, DHCP servers can also provide IP addresses for multiple subnets. In this case, a DHCP client that has not yet acquired an IP address cannot communicate directly with the DHCP server using IP routing, because it doesn't have a routable IP address, nor does it know the IP address of a router. In order to allow DHCP clients on subnets not directly served by DHCP servers to communicate with DHCP servers, DHCP relay agents can be installed on these subnets. The DHCP client broadcasts on the local link; the relay agent receives the broadcast and transmits it to one or more DHCP servers using unicast. The relay agent stores its own IP address in the GIADDR field of the DHCP packet. The DHCP server uses the GIADDR to determine the subnet on which the relay agent received the broadcast, and allocates an IP address on that subnet. When the DHCP server replies to the client, it sends the reply to the GIADDR address, again using unicast. The relay agent then retransmits the response on the local network.

## Reliability

The DHCP protocol provides reliability in several ways: periodic renewal, rebinding, and failover. DHCP clients are allocated leases that last for some period of time. Clients begin to attempt to renew their leases once half the lease interval has expired. They do this by sending a unicast DHCPREQUEST message to the DHCP server that granted the original lease. If that server is down or unreachable, it will fail to respond to the DHCPREQUEST. However, the DHCPREQUEST will be repeated by the client from time to time, so when the DHCP server comes back up or becomes reachable again, the DHCP client will succeed in contacting it, and renew its lease.

If the DHCP server is unreachable for an extended period of time, the DHCP client will attempt to rebinding, by broadcasting its DHCPREQUEST rather than unicasting it. Because it is broadcast, the DHCPREQUEST message will reach all available DHCP servers. If some other DHCP server is able to renew the lease, it will do so at this time.

In order for rebinding to work, when the client successfully contacts a backup DHCP server, that server must have accurate information about the client's binding. Maintaining accurate binding information between two servers is a complicated problem; if both servers are able to update the same lease database, there must be a mechanism to avoid conflicts between updates on the independent servers. A standard for implementing fault-tolerant DHCP servers was developed at the Internet Engineering Task Force.<sup>[16][17]</sup>

If rebinding fails, the lease will eventually expire. When the lease expires, the client must stop using the IP address granted to it in its lease. At that time, it will restart the DHCP process from the beginning by broadcasting a DHCPDISCOVER message. Since its lease has expired, it will accept any IP address offered to it. Once it has a new IP address, presumably from a different DHCP server, it will once again be able to use the network. However, since its IP address has changed, any ongoing connections will be broken.

## Security

The base DHCP protocol does not include any mechanism for authentication.<sup>[18]</sup> Because of this, it is vulnerable to a variety of attacks. These attacks fall into three main categories:

- Unauthorized DHCP servers providing false information to clients.<sup>[19]</sup>
- Unauthorized clients gaining access to resources.<sup>[19]</sup>
- Resource exhaustion attacks from malicious DHCP clients.<sup>[19]</sup>

Because the client has no way to validate the identity of a DHCP server, unauthorized DHCP servers can be operated on networks, providing incorrect information to DHCP clients. This can serve either as a denial-of-service attack, preventing the client from gaining access to network connectivity, or as a man-in-the-middle attack. Because the DHCP server provides the DHCP client with server IP addresses, such as the IP address of one or more DNS servers,<sup>[19]</sup> an attacker can convince a DHCP client to do its DNS lookups through its own DNS server, and can therefore provide its own answers to DNS queries from the client.<sup>[20]</sup> This in turn allows the attacker to redirect network traffic through itself, allowing it to eavesdrop on connections between the client and network servers it contacts, or to simply replace those network servers with its own.<sup>[20]</sup>

Because the DHCP server has no secure mechanism for authenticating the client, clients can gain unauthorized access to IP addresses by presenting credentials, such as client identifiers, that belong to other DHCP clients. This also allows DHCP clients to exhaust the DHCP server's store of IP addresses—by presenting new credentials each time it asks for an address, the client can consume all the available IP addresses on a particular network link, preventing other DHCP clients from getting service.

DHCP does provide some mechanisms for mitigating these problems. The Relay Agent Information Option protocol extension (RFC 3046) allows network operators to attach tags to DHCP messages as these messages arrive on the network operator's trusted network. This tag is then used as an authorization token to control the client's access to network resources. Because the client has no access to the network upstream of the relay agent, the lack of

authentication does not prevent the DHCP server operator from relying on the authorization token.<sup>[18]</sup>

Another extension, Authentication for DHCP Messages (RFC 3118), provides a mechanism for authenticating DHCP messages. Unfortunately RFC 3118 has not seen widespread adoption because of the problems of managing keys for large numbers of DHCP clients.<sup>[21]</sup>

## Notes

- [1] Ralph Droms; Ted Lemon (2003). *The DHCP Handbook*. SAMS Publishing. p. 436. ISBN 0-672-32327-3.
- [2] Bill Croft; John Gilmore (September 1985). "RFC 951 - Bootstrap Protocol" (<http://tools.ietf.org/html/rfc951#section-6>). *Network Working Group*.
- [3] <http://www.iana.org/assignments/bootp-dhcp-parameters>
- [4] In Unix-like systems this client-level refinement typically takes place according to the values in a `/etc/dhclient.conf` configuration file.
- [5] Alexander, Steve; Droms, Ralph (March 1997). *DHCP Options and BOOTP Vendor Extensions* (<https://tools.ietf.org/html/rfc2132>). IETF. RFC 2132. . Retrieved June 10, 2012.
- [6] Alexander, Steve; Droms, Ralph (March 1997). "RFC 2132: DHCP Options and BOOTP Vendor Extensions" (<http://tools.ietf.org/html/rfc2132#section-3>). IETF. Section 3: RFC 1497 vendor extensions. . Retrieved 2012-07-26.
- [7] Alexander, Steve; Droms, Ralph (March 1997). "RFC 2132: DHCP Options and BOOTP Vendor Extensions" (<http://tools.ietf.org/html/rfc2132#section-3.1>). IETF. Section 3.1: Pad Option. . Retrieved 2012-07-26.
- [8] Alexander, Steve; Droms, Ralph (March 1997). "RFC 2132: DHCP Options and BOOTP Vendor Extensions" (<http://tools.ietf.org/html/rfc2132#section-3.3>). IETF. Section 3.3: Subnet Mask. . Retrieved 2012-07-26.
- [9] Alexander, Steve; Droms, Ralph (March 1997). "RFC 2132: DHCP Options and BOOTP Vendor Extensions" (<http://tools.ietf.org/html/rfc2132#section-3.4>). IETF. Section 3.4: Time Offset. . Retrieved 2012-07-26.
- [10] Alexander, Steve; Droms, Ralph (March 1997). "RFC 2132: DHCP Options and BOOTP Vendor Extensions" (<http://tools.ietf.org/html/rfc2132#section-4>). IETF. Section 4: IP Layer Parameters per Host. . Retrieved 2012-07-26.
- [11] Alexander, Steve; Droms, Ralph (March 1997). "RFC 2132: DHCP Options and BOOTP Vendor Extensions" (<http://tools.ietf.org/html/rfc2132#section-5>). IETF. Section 5: IP Layer Parameters per Interface. . Retrieved 2012-07-26.
- [12] Alexander, Steve; Droms, Ralph (March 1997). "RFC 2132: DHCP Options and BOOTP Vendor Extensions" (<http://tools.ietf.org/html/rfc2132#section-6>). IETF. Section 6: Link Layer Parameters per Interface. . Retrieved 2012-07-26.
- [13] Alexander, Steve; Droms, Ralph (March 1997). "RFC 2132: DHCP Options and BOOTP Vendor Extensions" (<http://tools.ietf.org/html/rfc2132#section-7>). IETF. Section 7: TCP Parameters. . Retrieved 2012-07-26.
- [14] Alexander, Steve; Droms, Ralph (March 1997). "RFC 2132: DHCP Options and BOOTP Vendor Extensions" (<http://tools.ietf.org/html/rfc2132#section-8>). IETF. Section 8: Application and Service Parameters. . Retrieved 2012-07-26.
- [15] Alexander, Steve; Droms, Ralph (March 1997). "RFC 2132: DHCP Options and BOOTP Vendor Extensions" (<http://tools.ietf.org/html/rfc2132#section-9>). IETF. Section 9: DHCP Extensions. . Retrieved 2012-07-26.
- [16] Droms, Ralph; Kinnear, Kim; Stapp, Mark; Volz, Bernie; Gonczi, Steve; Rabil, Greg; Dooley, Michael; Kapur, Arun (March 2003). *DHCP Failover Protocol* (<https://tools.ietf.org/html/draft-ietf-dhc-failover-12>). IETF. I-D draft-ietf-dhc-failover-12. . Retrieved May 09, 2010.
- [17] The IETF proposal provided a mechanism whereby two servers could remain loosely in sync with each other in such a way that even in the event of a total failure of one server, the other server could recover the lease database and continue operating. Due to the length and complexity of the specification, it was never published as a standard; however, the techniques described in the specification are in wide use, with one open source implementation in the ISC DHCP server as well as several commercial implementations.
- [18] Michael Patrick (January 2001). "RFC 3046 - DHCP Relay Agent Information Option" (<http://tools.ietf.org/html/rfc3046#section-7>). *Network Working Group*.
- [19] Ralph Droms (March 1997). "RFC 2131 - Dynamic Host Configuration Protocol" (<http://tools.ietf.org/html/rfc2131#section-7>). *Network Working Group*.
- [20] Sergey Golovanov (Kaspersky Labs) (June 2011). "TDSS loader now got "legs"" ([http://www.securelist.com/en/blog/208188095/TDSS\\_loader\\_now\\_got\\_legs](http://www.securelist.com/en/blog/208188095/TDSS_loader_now_got_legs)). .
- [21] Ted Lemon (April 2002). "Implementation of RFC 3118" (<http://www.ietf.org/mail-archive/web/dhcwg/current/msg00876.html>). .

## References

### External links

- RFC 2131 - Dynamic Host Configuration Protocol
- RFC 2132 - DHCP Options and BOOTP Vendor Extensions
- RFC 3046 - DHCP Relay Agent Information Option
- RFC 3942 - Reclassifying Dynamic Host Configuration Protocol Version Four (DHCPv4) Options
- RFC 4242 - Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6
- RFC 4361 - Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
- RFC 4436 - Detecting Network Attachment in IPv4 (DNAv4)

## Network address translation

---

In computer networking, **network address translation (NAT)** is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.

The simplest type of NAT provides a one-to-one translation of IP addresses. RFC 2663 refers to this type of NAT as **basic NAT**. It is often also referred to as **one-to-one NAT**. In this type of NAT only the IP addresses, IP header checksum and any higher level checksums that include the IP address need to be changed. The rest of the packet can be left untouched (at least for basic TCP/UDP functionality, some higher level protocols may need further translation). Basic NATs can be used when there is a requirement to interconnect two IP networks with incompatible addressing.

However it is common to hide an entire IP address space, usually consisting of private IP addresses, behind a single IP address (or in some cases a small group of IP addresses) in another (usually public) address space. To avoid ambiguity in the handling of returned packets, a one-to-many NAT must alter higher level information such as TCP/UDP ports in outgoing communications and must maintain a translation table so that return packets can be correctly translated back. RFC 2663 uses the term **NAPT (network address and port translation)** for this type of NAT. Other names include **PAT (port address translation)**, **IP masquerading**, **NAT Overload** and **many-to-one NAT**. Since this is the most common type of NAT it is often referred to simply as NAT.

As described, the method enables communication through the router only when the conversation originates in the masqueraded network, since this establishes the translation tables. For example, a web browser in the masqueraded network can browse a website outside, but a web browser outside could not browse a web site in the masqueraded network. However, most NAT devices today allow the network administrator to configure translation table entries for permanent use. This feature is often referred to as "static NAT" or port forwarding and allows traffic originating in the "outside" network to reach designated hosts in the masqueraded network.

In the mid-1990s NAT became a popular tool for alleviating the consequences of IPv4 address exhaustion.<sup>[1]</sup> It has become a common, indispensable feature in routers for home and small-office Internet connections. Most systems using NAT do so in order to enable multiple hosts on a private network to access the Internet using a single public IP address.

Network address translation has serious drawbacks on the quality of Internet connectivity and requires careful attention to the details of its implementation. In particular, all types of NAT break the originally envisioned model of IP end-to-end connectivity across the Internet and NAPT makes it difficult for systems behind a NAT to accept incoming communications. As a result, NAT traversal methods have been devised to alleviate the issues encountered.

## One-to-many NATs

The majority of NATs map multiple private hosts to one publicly exposed IP address. In a typical configuration, a local network uses one of the designated "private" IP address subnets (RFC 1918). A router on that network has a private address in that address space. The router is also connected to the Internet with a "public" address assigned by an Internet service provider. As traffic passes from the local network to the Internet, the source address in each packet is translated on the fly from a private address to the public address. The router tracks basic data about each active connection (particularly the destination address and port). When a reply returns to the router, it uses the connection tracking data it stored during the outbound phase to determine the private address on the internal network to which to forward the reply.

All Internet packets have a source IP address and a destination IP address. Typically packets passing from the private network to the public network will have their source address modified while packets passing from the public network back to the private network will have their destination address modified. More complex configurations are also possible.

To avoid ambiguity in how to translate returned packets, further modifications to the packets are required. The vast bulk of Internet traffic is TCP and UDP packets, and for these protocols the port numbers are changed so that the combination of IP and port information on the returned packet can be unambiguously mapped to the corresponding private address and port information. Protocols not based on TCP or UDP require other translation techniques. ICMP packets typically relate to an existing connection and need to be mapped using the same IP and port mappings as that connection.

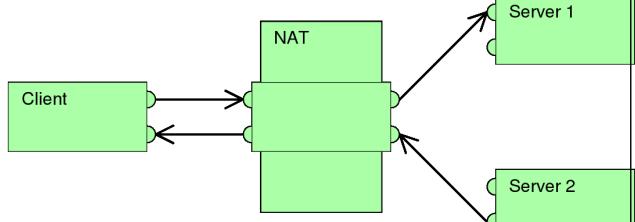
## Methods of Port translation

There are several ways of implementing network address and port translation. In some application protocols that use IP address information, the application running on a node in the masqueraded network needs to determine the external address of the NAT, i.e., the address that its communication peers detect, and, furthermore, often needs to examine and categorize the type of mapping in use. Usually this is done because it is desired to set up a direct communications path (either to save the cost of taking the data via a server or to improve performance) between two clients both of which are behind separate NATs. For this purpose, the Simple traversal of UDP over NATs (STUN) protocol was developed (RFC 3489, March 2003). It classified NAT implementation as *full cone NAT*, *address restricted cone NAT*, *port restricted cone NAT* or *symmetric NAT* and proposed a methodology for testing a device accordingly. However, these procedures have since been deprecated from standards status, as the methods have proven faulty and inadequate to correctly assess many devices. New methods have been standardized in RFC 5389 (October 2008) and the STUN acronym now represents the new title of the specification: *Session Traversal Utilities for NAT*.

### Full-cone NAT, also known as *one-to-one NAT*

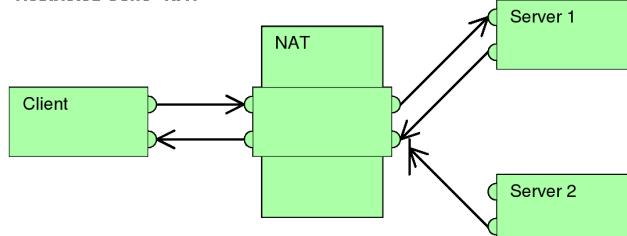
- Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
- Any external host* can send packets to iAddr:iPort by sending packets to eAddr:ePort.

**"Full Cone" NAT**



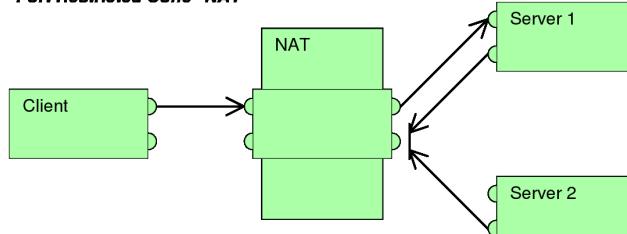
**(Address) restricted cone NAT**

- Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
- An external host (*hAddr:any*) can send packets to iAddr:iPort by sending packets to eAddr:ePort only if iAddr:iPort has previously sent a packet to hAddr:*any*. "Any" means the port number doesn't matter.

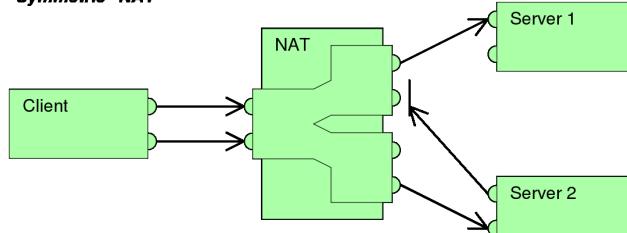
**"Restricted Cone" NAT****Port-restricted cone NAT**

Like an address restricted cone NAT, but the restriction includes port numbers.

- Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
- An external host (*hAddr:hPort*) can send packets to iAddr:iPort by sending packets to eAddr:ePort only if iAddr:iPort has previously sent a packet to hAddr:hPort.

**"Port Restricted Cone" NAT****Symmetric NAT**

- Each request from the same internal IP address and port to a specific destination IP address and port is mapped to a unique external source IP address and port, if the same internal host sends a packet even with the same source address and port but to a different destination, a different mapping is used.
- Only an external host that receives a packet from an internal host can send a packet back.

**"Symmetric" NAT**

This terminology has been the source of much confusion, as it has proven inadequate at describing real-life NAT behavior.<sup>[2]</sup> Many NAT implementations combine these types, and it is therefore better to refer to specific individual NAT behaviors instead of using the Cone/Symmetric terminology. Especially, most NAT translators combine *symmetric NAT* for outgoing connections with *static port mapping*, where incoming packets to the external address and port are redirected to a specific internal address and port. Some products can redirect packets to several internal hosts, e.g. to divide the load between a few servers. However, this introduces problems with more sophisticated communications that have many interconnected packets, and thus is rarely used.

## Type of NAT and NAT Traversal

The NAT traversal problem arises when two peers behind distinct NAT try to communicate. One way to solve this problem is to use port forwarding, another way is to use various NAT traversal techniques. The most popular technique for TCP NAT traversal is TCP hole punching, which requires the NAT to follow the *port preservation* design for TCP, as explained below.

Many NAT implementations follow the *port preservation* design especially for TCP, which is to say that they use the same values as internal and external port numbers. NAT *port preservation* for outgoing TCP connections is especially important for TCP NAT traversal, because programs usually bind distinct TCP sockets to ephemeral ports for distinct TCP connections, rendering NAT port prediction impossible for TCP.

On the other hand, for UDP, NATs do not need to have *port preservation* because applications usually reuse the same UDP socket to send packets to distinct hosts, making port prediction straightforward, as it is the same source port for each packet.

Furthermore, *port preservation* in NAT for TCP allows P2P protocols to offer less complexity and less latency because there is no need to use a third party to discover the NAT port since the application already knows the NAT port.<sup>[3]</sup>

However, if two internal hosts attempt to communicate with the same external host using the same port number, the external port number used by the second host will be chosen at random. Such NAT will be sometimes perceived as (*address*) *restricted cone NAT* and other times as *symmetric NAT*.

Recent studies have shown that roughly 70% of clients in P2P networks employ some form of NAT.<sup>[4]</sup>

## Implementation

### Establishing Two-Way Communication

Every TCP and UDP packet contains both a source IP address and source port number as well as a destination IP address and destination port number. The port address/IP address pair forms a socket. In particular, the source port address and source IP address form the source socket.

For publicly accessible services such as web servers and mail servers the port number is important. For example, port 80 connects to the web server software and port 25 to a mail server's SMTP daemon. The IP address of a public server is also important, similar in global uniqueness to a postal address or telephone number. Both IP address and port must be correctly known by all hosts wishing to successfully communicate.

Private IP addresses as described in RFC 1918 are significant only on private networks where they are used, which is also true for host ports. Ports are unique endpoints of communication on a host, so a connection through the NAT device is maintained by the combined mapping of port and IP address.

PAT (Port Address Translation) resolves conflicts that would arise through two different hosts using the same source port number to establish unique connections at the same time.

### An Analogy

A NAT device is similar to a phone system at an office that has one public telephone number and multiple extensions. Outbound phone calls made from the office all appear to come from the same telephone number. However, an incoming call that does not specify an extension cannot be transferred to an individual inside the office. In this scenario, the office is a private LAN, the main phone number is the public IP address, and the individual extensions are unique port numbers.<sup>[5]</sup>

## Translation of the Endpoint

With NAT, all communication sent to external hosts actually contain the *external IP* address and port information of the NAT device instead of internal host IPs or port numbers.

- When a computer on the private (internal) network sends a packet to the external network, the NAT device replaces the internal IP address in the source field of the packet header (*sender's address*) with the external IP address of the NAT device. PAT may then assign the connection a port number from a pool of available ports, inserting this port number in the source port field (much like the *post office box number*), and forwards the packet to the external network. The NAT device then makes an entry in a translation table containing the internal IP address, original source port, and the translated source port. Subsequent packets from the same connection are translated to the same port number.
- The computer receiving a packet that has undergone NAT establishes a connection to the port and IP address specified in the altered packet, oblivious to the fact that the supplied address is being translated (analogous to using a *post office box number*).
- A packet coming from the external network is mapped to a corresponding internal IP address and port number from the translation table, replacing the external IP address and port number in the incoming packet header (similar to the translation from *post office box number* to *street address*). The packet is then forwarded over the inside network. Otherwise, if the destination port number of the incoming packet is not found in the translation table, the packet is dropped or rejected because the PAT device doesn't know where to send it.

NAT will only translate IP addresses and ports of its internal hosts, hiding the true endpoint of an internal host on a private network.

## Visibility of Operation

NAT operation is typically transparent to both the internal and external hosts.

Typically the internal host is aware of the true IP address and TCP or UDP port of the external host. Typically the NAT device may function as the default gateway for the internal host. However the external host is only aware of the public IP address for the NAT device and the particular port being used to communicate on behalf of a specific internal host.

## NAT and TCP/UDP

"Pure NAT", operating on IP alone, may or may not correctly parse protocols that are totally concerned with IP information, such as ICMP, depending on whether the payload is interpreted by a host on the "inside" or "outside" of translation. As soon as the protocol stack is traversed, even with such basic protocols as TCP and UDP, the protocols will break unless NAT takes action beyond the network layer.

IP packets have a checksum in each packet header, which provides error detection only for the header. IP datagrams may become fragmented and it is necessary for a NAT to reassemble these fragments to allow correct recalculation of higher-level checksums and correct tracking of which packets belong to which connection.

The major transport layer protocols, TCP and UDP, have a checksum that covers all the data they carry, as well as the TCP/UDP header, plus a "pseudo-header" that contains the source and destination IP addresses of the packet carrying the TCP/UDP header. For an originating NAT to pass TCP or UDP successfully, it must recompute the TCP/UDP header checksum based on the translated IP addresses, not the original ones, and put that checksum into the TCP/UDP header of the first packet of the fragmented set of packets. The receiving NAT must recompute the IP checksum on every packet it passes to the destination host, and also recognize and recompute the TCP/UDP header using the retranslated addresses and pseudo-header. This is not a completely solved problem. One solution is for the receiving NAT to reassemble the entire segment and then recompute a checksum calculated across all packets.

---

The originating host may perform Maximum transmission unit (MTU) path discovery to determine the packet size that can be transmitted without fragmentation, and then set the *don't fragment* (DF) bit in the appropriate packet header field.

## Destination network address translation (DNAT)

DNAT is a technique for transparently changing the destination IP address of an en-route packet and performing the inverse function for any replies. Any router situated between two endpoints can perform this transformation of the packet.

DNAT is commonly used to publish a service located in a private network on a publicly accessible IP address. This use of DNAT is also called port forwarding, or DMZ when used on an entire server, which becomes exposed to the WAN, becoming analogous to an undefended military demilitarised zone (DMZ).

## SNAT

The meaning of the term *SNAT* varies by vendor. Many vendors have proprietary definitions for *SNAT*. A common expansion is *source NAT*, the counterpart of *destination NAT (DNAT)*. Microsoft uses the acronym for *Secure NAT*, in regard to the ISA Server. For Cisco Systems, *SNAT* means *stateful NAT*. For Watchguard Systems, *SNAT* means *static NAT*.

## Secure network address translation

In computer networking, the process of network address translation done in a secure way involves rewriting the source and/or destination addresses of IP packets as they pass through a router or firewall.

## Dynamic network address translation

Dynamic NAT, just like static NAT, is not common in smaller networks but is found within larger corporations with complex networks. The way dynamic NAT differs from static NAT is that where static NAT provides a one-to-one internal to public static IP address mapping, dynamic NAT doesn't make the mapping to the public IP address static and usually uses a group of available public IP addresses.

## Applications affected by NAT

Some Application Layer protocols (such as FTP and SIP) send explicit network addresses within their application data. FTP in active mode, for example, uses separate connections for control traffic (commands) and for data traffic (file contents). When requesting a file transfer, the host making the request identifies the corresponding data connection by its network layer and transport layer addresses. If the host making the request lies behind a simple NAT firewall, the translation of the IP address and/or TCP port number makes the information received by the server invalid. The Session Initiation Protocol (SIP) controls many Voice over IP (VoIP) calls, and suffers the same problem. SIP and SDP may use multiple ports to set up a connection and transmit voice stream via RTP. IP addresses and port numbers are encoded in the payload data and must be known prior to the traversal of NATs. Without special techniques, such as STUN, NAT behavior is unpredictable and communications may fail.

Application layer gateway (ALG) software or hardware may correct these problems. An ALG software module running on a NAT firewall device updates any payload data made invalid by address translation. ALGs obviously need to understand the higher-layer protocol that they need to fix, and so each protocol with this problem requires a separate ALG. For example, on many Linux systems, there are kernel modules called *connection trackers* which serve to implement ALGs. However, ALG does not work if the control channel is encrypted (e.g. FTPS).

Another possible solution to this problem is to use NAT traversal techniques using protocols such as STUN or ICE, or proprietary approaches in a session border controller. NAT traversal is possible in both TCP- and UDP-based applications, but the UDP-based technique is simpler, more widely understood, and more compatible with legacy NATs. In either case, the high level protocol must be designed with NAT traversal in mind, and it does not work reliably across symmetric NATs or other poorly behaved legacy NATs.

Other possibilities are UPnP (Universal Plug and Play) or NAT-PMP (NAT Port Mapping Protocol), but these require the cooperation of the NAT device.

Most traditional client-server protocols (FTP being the main exception), however, do not send layer 3 contact information and therefore do not require any special treatment by NATs. In fact, avoiding NAT complications is practically a requirement when designing new higher-layer protocols today (e.g. the use of SFTP instead of FTP).

NATs can also cause problems where IPsec encryption is applied and in cases where multiple devices such as SIP phones are located behind a NAT. Phones which encrypt their signaling with IPsec encapsulate the port information within an encrypted packet, meaning that NA(P)T devices cannot access and translate the port. In these cases the NA(P)T devices revert to simple NAT operation. This means that all traffic returning to the NAT will be mapped onto one client causing service to more than one client "behind" the NAT to fail. There are a couple of solutions to this problem: one is to use TLS, which operates at level 4 in the OSI Reference Model and therefore does not mask the port number; another is to encapsulate the IPsec within UDP - the latter being the solution chosen by TISPAN to achieve secure NAT traversal.

The DNS protocol vulnerability announced by Dan Kaminsky on July 8, 2008 is indirectly affected by NAT port mapping. To avoid DNS server cache poisoning, it is highly desirable to not translate UDP source port numbers of outgoing DNS requests from a DNS server which is behind a firewall which implements NAT. The recommended work-around for the DNS vulnerability is to make all caching DNS servers use randomized UDP source ports. If the NAT function de-randomizes the UDP source ports, the DNS server will be made vulnerable.

## Advantages of PAT

In addition to the advantages provided by NAT:

- PAT (Port Address Translation) allows many internal hosts to share a single external IP address.
- Users who do not require support for inbound connections do not consume public IP addresses.

## Drawbacks

The primary purpose of IP-masquerading NAT is that it has been a practical solution to the impending exhaustion of IPv4 address space. Even large networks can be connected to the Internet with as little as a single IP address. The more common arrangement is having machines that require end-to-end connectivity supplied with a routable IP address, while having machines that do not provide services to outside users behind NAT with only a few IP addresses used to enable Internet access, however, this brings some problems, outlined below.

Some<sup>[6]</sup> have also called this exact feature a major drawback, since it delays the need for the implementation of IPv6:

"[...] it is possible that its [NAT's] widespread use will significantly delay the need to deploy IPv6. [...] It is probably safe to say that networks would be better off without NAT [...]"

Hosts behind NAT-enabled routers do not have end-to-end connectivity and cannot participate in some Internet protocols. Services that require the initiation of TCP connections from the outside network, or stateless protocols such as those using UDP, can be disrupted. Unless the NAT router makes a specific effort to support such protocols, incoming packets cannot reach their destination. Some protocols can accommodate one instance of NAT between participating hosts ("passive mode" FTP, for example), sometimes with the assistance of an application-level gateway (see below), but fail when both systems are separated from the Internet by NAT. Use of NAT also

complicates tunneling protocols such as IPsec because NAT modifies values in the headers which interfere with the integrity checks done by IPsec and other tunneling protocols.

End-to-end connectivity has been a core principle of the Internet, supported for example by the Internet Architecture Board. Current Internet architectural documents observe that NAT is a violation of the End-to-End Principle, but that NAT does have a valid role in careful design.<sup>[7]</sup> There is considerably more concern with the use of IPv6 NAT, and many IPv6 architects believe IPv6 was intended to remove the need for NAT.<sup>[8]</sup>

Because of the short-lived nature of the stateful translation tables in NAT routers, devices on the internal network lose IP connectivity typically within a very short period of time unless they implement NAT keep-alive mechanisms by frequently accessing outside hosts. This dramatically shortens the power reserves on battery-operated hand-held devices and has thwarted more widespread deployment of such IP-native Internet-enabled devices.

Some Internet service providers (ISPs), especially in India, Russia, parts of Asia and other "developing" regions provide their customers only with "local" IP addresses, due to a limited number of external IP addresses allocated to those entities. Thus, these customers must access services external to the ISP's network through NAT. As a result, the customers cannot achieve true end-to-end connectivity, in violation of the core principles of the Internet as laid out by the Internet Architecture Board.

- Scalability - An implementation that only tracks ports can be quickly depleted by internal applications that use multiple simultaneous connections (such as an HTTP request for a web page with many embedded objects). This problem can be mitigated by tracking the destination IP address in addition to the port (thus sharing a single local port with many remote hosts), at the expense of implementation complexity and CPU/memory resources of the translation device.
- Firewall complexity - Because the internal addresses are all disguised behind one publicly accessible address, it is impossible for external hosts to initiate a connection to a particular internal host without special configuration on the firewall to forward connections to a particular port. Applications such as VOIP, videoconferencing, and other peer-to-peer applications must use NAT traversal techniques to function.

## Specifications

IEEE<sup>[9]</sup> Reverse Address and Port Translation (RAPT, or RAT) allows a host whose real IP address is changing from time to time to remain reachable as a server via a fixed home IP address. In principle, this should allow setting up servers on DHCP-run networks. While not a perfect mobility solution, RAPT together with upcoming protocols like DHCP-DDNS, it may end up becoming another useful tool in the network admin's arsenal.

IETF<sup>[10]</sup> *RAPT* (IP Reachability Using Twice Network Address and Port Translation) The RAT device maps an IP datagram to its associated CN and OMN by using three additional fields: the IP protocol type number and the transport layer source and destination connection identifiers (e.g. TCP port number or ICMP echo request/reply ID field).

Cisco *RAPT* implementation is PAT (Port Address Translation) or overloading, and maps multiple private IP addresses to a single public IP address. Multiple addresses can be mapped to a single address because each private address is tracked by a port number. PAT uses unique source port numbers on the inside global IP address to distinguish between translations. The port number is encoded in 16 bits. The total number of internal addresses that can be translated to one external address could theoretically be as high as 65,536 per IP address. Realistically, the number of ports that can be assigned a single IP address is around 4000. PAT will attempt to preserve the original source port. If this source port is already used, PAT will assign the first available port number starting from the beginning of the appropriate port group 0-511, 512-1023, or 1024-65535. When there are no more ports available and there is more than one external IP address configured, PAT moves to the next IP address to try to allocate the original source port again. This process continues until it runs out of available ports and external IP addresses.

**3COM U.S. Patent 6055236** [11] (Method and system for locating network services with distributed network address translation) Methods and system for locating network services with distributed network address translation. Digital certificates are created that allow an external network device on an external network, such as the Internet, to request a service from an internal network device on an internal distributed network address translation network, such as a stub local area network. The digital certificates include information obtained with a Port Allocation Protocol used for distributed network address translation. The digital certificates are published on the internal network so they are accessible to external network devices. An external network device retrieves a digital certificate, extracts appropriate information, and sends a service request packet to an internal network device on an internal distributed network address translation network. The external network device is able to locate and request a service from an internal network device. An external network device can also request a security service, such as an Internet Protocol security ("IPsec") service from an internal network device. The external network device and the internal network device can establish a security service (e.g., Internet Key Exchange protocol service). The internal network device and external network device can then establish a Security Association using Security Parameter Indexes ("SPI") obtained using a distributed network address translation protocol. External network devices can request services, and security services on internal network devices on an internal distribute network address translation network that were previously unknown and unavailable to the external network devices.

## Examples of NAT software

- Internet Connection Sharing (ICS): Windows NAT+DHCP since W98SE
- WinGate: like ICS plus lots of control
- iptables: the Linux packet filter and NAT (interface for NetFilter)
- IPFilter: Solaris, NetBSD, FreeBSD, xMach.
- PF (firewall): The OpenBSD Packet Filter.
- Netfilter Linux packet filter framework

## References

- [1] [www.tcpipguide.com/free/t\\_IPNetworkAddressTranslationNATProtocol.htm](http://www.tcpipguide.com/free/t_IPNetworkAddressTranslationNATProtocol.htm) ([http://www.tcpipguide.com/free/t\\_IPNetworkAddressTranslationNATProtocol.htm](http://www.tcpipguide.com/free/t_IPNetworkAddressTranslationNATProtocol.htm))
- [2] François Audet; and Cullen Jennings (January 2007) (text). *RFC 4787 Network Address Translation (NAT) Behavioral Requirements for Unicast UDP* (<http://www.ietf.org/rfc/rfc4787.txt>). IETF. . Retrieved 2007-08-29.
- [3] "Characterization and Measurement of TCP Traversal through NATs and Firewalls" (<http://nutss.gforge.cis.cornell.edu/pub/imc05-tcpnat/>). December 2006. .
- [4] "Illuminating the shadows: Opportunistic network and web measurement" (<http://illuminati.coralcdn.org/stats/>). December 2006. .
- [5] "The Audio over IP Instant Expert Guide" (<http://www.tieline.com/Downloads/Audio-over-IP-Instant-Expert-Guide-v1.pdf>). Tieline. January 2010. . Retrieved 2011-08-19.
- [6] Larry L. Peterson; and Bruce S. Davie; *Computer Networks: A Systems Approach*, Morgan Kaufmann, 2003, pp. 328-330, ISBN 1-55860-832-X
- [7] R. Bush; and D. Meyer; RFC 3439, *Some Internet Architectural Guidelines and Philosophy* (<http://www.ietf.org/rfc/rfc3439.txt>), December 2002
- [8] G. Van de Velde *et al.*; RFC 4864, *Local Network Protection for IPv6* (<http://tools.ietf.org/rfc/rfc4864.txt>), May 2007
- [9] <http://ieeexplore.ieee.org/iel4/6056/16183/00749275.pdf>
- [10] <http://www3.ietf.org/proceedings/99nov/I-D/draft-ietf-nat-rnat-00.txt>
- [11] <http://www.google.com/patents?vid=6055236>

## External links

- NAT-Traversal Test and results (<http://nattest.net.in.tum.de>)
- Characterization of different TCP NATs (<http://nutss.net/pub/imc05-tcpnat/>) – Paper discussing the different types of NAT
- Anatomy: A Look Inside Network Address Translators – Volume 7, Issue 3, September 2004 ([http://www.cisco.com/en/US/about/ac123/ac147/archived\\_issues/ipj\\_7-3/anatomy.html](http://www.cisco.com/en/US/about/ac123/ac147/archived_issues/ipj_7-3/anatomy.html))
- Jeff Tyson, HowStuffWorks: *How Network Address Translation Works* (<http://computer.howstuffworks.com/nat.htm/printable>)
- NAT traversal techniques in multimedia Networks (<http://www.newport-networks.com/whitepapers/nat-traversal1.html>) – White Paper from Newport Networks
- NAT traversal for IP Communications (<http://www.voiptraversal.com/EyeballAnyfirewallWhitePaper.pdf>) – White Paper from Eyeball Networks
- Peer-to-Peer Communication Across Network Address Translators (<http://www.brynosaurus.com/pub/net/p2pnat/>) (PDF) (<http://www.brynosaurus.com/pub/net/p2pnat.pdf>) – NAT traversal techniques for UDP and TCP
- <http://www.zdnetasia.com/insight/network/0,39044847,39050002,00.htm>
- RFCs
  - RFC 1631 (Status: Obsolete) - The IP Network Address Translator (NAT)
  - RFC 1918 - Address Allocation for Private Internets
  - RFC 3022 (Status: Informational) – Traditional IP Network Address Translator (Traditional NAT)
  - RFC 4008 (Status: Standards Track) – Definitions of Managed Objects for Network Address Translators (NAT)
  - RFC 5128 (Status: Informational) - State of Peer-to-Peer (P2P) Communications across Network Address Translators (NATs)
  - RFC 4966 (Status: Informational) - Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status
- *Speak Freely* End of Life Announcement (<http://www.fourmilab.ch/speakfree/unix/>) – John Walker's discussion of why he stopped developing a famous program for free Internet communication, part of which is directly related to NAT
- natd ([http://www.freebsd.org/doc/en\\_US.ISO8859-1/books/handbook/network-natd.html](http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-natd.html))
- SNAT, DNAT and OCS2007R2 (<http://www.cainetworks.com/support/training/snat-dnat-ocs.html>) – discussing the SNAT in Microsoft OCS 2007R2
- Alternative Taxonomy (Part of the documentation for the IBM iSeries)
  - Static NAT (<http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzajw/rzajwstatic.htm>)
  - Dynamic NAT (<http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzajw/rzajwdynamic.htm>)
  - Masquerade NAT (<http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzajw/rzajwaddmasq.htm>)
- Network Address Translation - NAT (<http://blog.ipexpert.com/2009/09/07/network-address-translation-nat/>)
- Cisco Systems
  - Document ID 6450: How NAT Works ([http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080094831.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml))
  - Document ID 26704: Network Address Translation (NAT) FAQ ([http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_q\\_and\\_a\\_item09186a00800e523b.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_q_and_a_item09186a00800e523b.shtml))

- White Paper: Cisco IOS Network Address Translation Overview ([http://www.cisco.com/en/US/technologies/tk648/tk361/tk438/technologies\\_white\\_paper09186a0080091cb9.html](http://www.cisco.com/en/US/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html))
- Cisco IOS NAT Commands Cisco IOS commands (<http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/cs/csprtd/csprtd11/csnat.htm>)
- Animation Cisco NAT sample (<http://www.cisco.com/image/gif/paws/6450/nat.swf>)

# Simple Network Management Protocol

## SNMP (Simple Network Management Protocol)

Port(s)	161, 162, 10161, 10162
---------	------------------------

**Simple Network Management Protocol (SNMP)** is an "Internet-standard protocol for managing devices on IP networks." Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more.<sup>[1]</sup> It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.<sup>[2]</sup>

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

## Overview and basic concepts

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an *agent* which reports information via SNMP to the manager.

Essentially, SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

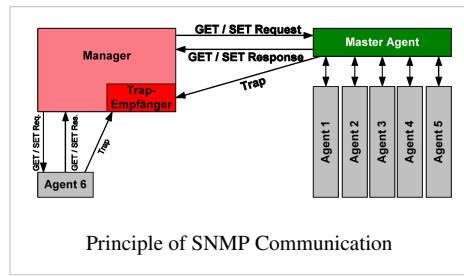
An SNMP-managed network consists of three key components:

- Managed device
- Agent — software which runs on managed devices
- Network management system (NMS) — software which runs on the manager

A *managed device* is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An *agent* is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP specific form.

A *network management system* (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.



## Management information base (MIB)

SNMP itself does not define which information (which variables) a managed system should offer. Rather, SNMP uses an extensible design, where the available information is defined by management information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP. MIBs use the notation defined by ASN.1.

## Protocol details

SNMP operates in the Application Layer of the Internet Protocol Suite (Layer 7 of the OSI model). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications (*Traps* and *InformRequests*) on port 162. The agent may generate notifications from any available port. When used with Transport Layer Security or Datagram Transport Layer Security requests are received on port 10161 and traps are sent to port 10162.<sup>[3]</sup>.

SNMPv1 specifies five core protocol data units (PDUs). Two other PDUs, *GetBulkRequest* and *InformRequest* were added in SNMPv2 and carried over to SNMPv3.

All SNMP PDUs are constructed as follows:

IP header	UDP header	version	community	PDU-type	request-id	error-status	error-index	variable bindings
-----------	------------	---------	-----------	----------	------------	--------------	-------------	-------------------

The seven SNMP protocol data units (PDUs) are as follows:

### GetRequest

A **manager-to-agent** request to retrieve the value of a variable or list of variables. Desired variables are specified in variable bindings (values are not used). Retrieval of the specified variable values is to be done as an atomic operation by the agent. A *Response* with current values is returned.

### SetRequest

A **manager-to-agent** request to change the value of a variable or list of variables. Variable bindings are specified in the body of the request. Changes to all specified variables are to be made as an atomic operation by the agent. A *Response* with (current) new values for the variables is returned.

### GetNextRequest

A **manager-to-agent** request to discover available variables and their values. Returns a *Response* with variable binding for the lexicographically next variable in the MIB. The entire MIB of an agent can be walked by iterative application of *GetNextRequest* starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.

### GetBulkRequest

Optimized version of *GetNextRequest*. A **manager-to-agent** request for multiple iterations of *GetNextRequest*. Returns a *Response* with multiple variable bindings walked from the variable binding or bindings in the request. PDU specific *non-repeaters* and *max-repetitions* fields are used to control response behavior. *GetBulkRequest* was introduced in SNMPv2.

## Response

Returns variable bindings and acknowledgement from **agent to manager** for *GetRequest*, *SetRequest*, *GetNextRequest*, *GetBulkRequest* and *InformRequest*. Error reporting is provided by *error-status* and *error-index* fields. Although it was used as a response to both gets and sets, this PDU was called *GetResponse* in SNMPv1.

## Trap

Asynchronous notification from **agent to manager**. Includes current *sysUpTime* value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed *SNMPv2-Trap*.

## InformRequest

Acknowledged asynchronous notification **manager to manager**<sup>[4]</sup> or agent to manager. Manager-to-manager notifications were already possible in SNMPv1 (using a *Trap*), but as SNMP commonly runs over UDP where delivery is not assured and dropped packets are not reported, delivery of a *Trap* was not guaranteed. *InformRequest* fixes this by sending back an acknowledgement on receipt. Receiver replies with *Response* parroting all information in the *InformRequest*. This PDU was introduced in SNMPv2.<sup>[5]</sup>

## Development and usage

### Version 1

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX). SNMPv1 is widely used and is the de facto network-management protocol in the Internet community.

The first RFCs for SNMP, now known as SNMPv1, appeared in 1988:

- RFC 1065 — Structure and identification of management information for TCP/IP-based internets
- RFC 1066 — Management information base for network management of TCP/IP-based internets
- RFC 1067 — A simple network management protocol

These protocols were obsoleted by:

- RFC 1155 — Structure and identification of management information for TCP/IP-based internets
- RFC 1156 — Management information base for network management of TCP/IP-based internets
- RFC 1157 — A simple network management protocol

After a short time, RFC 1156 (MIB-1) was replaced by more often used:

- RFC 1213 — Version 2 of management information base (MIB-2) for network management of TCP/IP-based internets

Version 1 has been criticized for its poor security.<sup>[6]</sup> Authentication of clients is performed only by a "community string", in effect a type of password, which is transmitted in cleartext. The '80s design of SNMP V1 was done by a group of collaborators who viewed the officially sponsored OSI/IETF/NSF (National Science Foundation) effort (HEMS/CMIS/CMIP) as both unimplementable in the computing platforms of the time as well as potentially unworkable. SNMP was approved based on a belief that it was an interim protocol needed for taking steps towards large scale deployment of the Internet and its commercialization. In that time period Internet-standard authentication/security was both a dream and discouraged by focused protocol design groups.

## Version 2

SNMPv2 (RFC 1441–RFC 1452), revises version 1 and includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. It introduced *GetBulkRequest*, an alternative to iterative GetNextRequests for retrieving large amounts of management data in a single request. However, the new party-based security system in SNMPv2, viewed by many as overly complex, was not widely accepted.<sup>[6]</sup>

*Community-Based Simple Network Management Protocol version 2*, or *SNMPv2c*, is defined in RFC 1901–RFC 1908. In its initial stages, this was also informally known as *SNMPv1.5*. SNMPv2c comprises SNMPv2 *without* the controversial new SNMP v2 security model, using instead the simple community-based security scheme of SNMPv1. While officially only a "Draft Standard", this is widely considered the *de facto* SNMPv2 standard.

*User-Based Simple Network Management Protocol version 2*, or *SNMPv2u*, is defined in RFC 1909–RFC 1910. This is a compromise that attempts to offer greater security than SNMPv1, but without incurring the high complexity of SNMPv2. A variant of this was commercialized as *SNMP v2\**, and the mechanism was eventually adopted as one of two security frameworks in SNMP v3.

## SNMPv1 & SNMPv2c interoperability

As presently specified, SNMPv2c is incompatible with SNMPv1 in two key areas: message formats and protocol operations. SNMPv2c messages use different header and protocol data unit (PDU) formats from SNMPv1 messages. SNMPv2c also uses two protocol operations that are not specified in SNMPv1. Furthermore, RFC 2576 defines two possible SNMPv1/v2c coexistence strategies: proxy agents and bilingual network-management systems.

### Proxy agents

A SNMPv2 agent can act as a proxy agent on behalf of SNMPv1 managed devices, as follows:

- A SNMPv2 NMS issues a command intended for a SNMPv1 agent.
- The NMS sends the SNMP message to the SNMPv2 proxy agent.
- The proxy agent forwards Get, GetNext, and Set messages to the SNMPv1 agent unchanged.
- GetBulk messages are converted by the proxy agent to GetNext messages and then are forwarded to the SNMPv1 agent.

The proxy agent maps SNMPv1 trap messages to SNMPv2 trap messages and then forwards them to the NMS.

### Bilingual network-management system

Bilingual SNMPv2 network-management systems support both SNMPv1 and SNMPv2. To support this dual-management environment, a management application in the bilingual NMS must contact an agent. The NMS then examines information stored in a local database to determine whether the agent supports SNMPv1 or SNMPv2. Based on the information in the database, the NMS communicates with the agent using the appropriate version of SNMP.

## Version 3

Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security, it looks much different due to new textual conventions, concepts, and terminology.<sup>[1]</sup>

SNMPv3 primarily added security and remote configuration enhancements to SNMP.<sup>[7]</sup>

Security has been the biggest weakness of SNMP since the beginning. Authentication in SNMP Versions 1 and 2 amounts to nothing more than a password (community string) sent in clear text between a manager and agent.<sup>[1]</sup> Each SNMPv3 message contains security parameters which are encoded as an octet string. The meaning of these security parameters depends on the security model being used.<sup>[8]</sup>

SNMPv3 provides important security features:<sup>[9]</sup>

- Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.
- Integrity - Message integrity to ensure that a packet has not been tampered with in transit including an optional packet replay protection mechanism.
- Authentication - to verify that the message is from a valid source.

As of 2004 the IETF recognizes *Simple Network Management Protocol version 3* as defined by RFC 3411–RFC 3418<sup>[10]</sup> (also known as STD0062) as the current standard version of SNMP. The IETF has designated SNMPv3 a full Internet standard,<sup>[11]</sup> the highest maturity level for an RFC. It considers earlier versions to be obsolete (designating them "Historic").<sup>[12]</sup>

In practice, SNMP implementations often support multiple versions: typically SNMPv1, SNMPv2c, and SNMPv3.<sup>[13]</sup>

## Implementation issues

SNMP implementations vary across platform vendors. In some cases, SNMP is an added feature, and is not taken seriously enough to be an element of the core design. Some major equipment vendors tend to over-extend their proprietary command line interface (CLI) centric configuration and control systems.<sup>[14]</sup>

SNMP's seemingly simple tree structure and linear indexing may not always be understood well enough within the internal data structures that are elements of a platform's basic design. Consequently, processing SNMP queries on certain data sets may result in higher CPU utilization than necessary. One example of this would be large routing tables, such as BGP or IGP.

## Resource indexing

Modular devices may dynamically increase or decrease their SNMP indices (aka instances) whenever slotted hardware is added or removed. Although this is most common with hardware, virtual interfaces have the same effect. Index values are typically assigned at boot time and remain fixed until the next reboot. Hardware or virtual entities added while the device is 'live' may have their indices assigned at the end of the existing range and possibly reassigned at the next reboot. Network inventory and monitoring tools need to have the device update capability by properly reacting to the cold start trap from the device reboot in order to avoid corruption and mismatch of polled data.

Index assignments for an SNMP device instance may change from poll to poll mostly as a result of changes initiated by the system admin. If information is needed for a particular interface, it is imperative to determine the SNMP index before retrieving the data needed. Generally, a description table like ifDescr will map a user friendly name like Serial 0/1 (Blade 0, port 1) to an SNMP index.

## Security implications

- SNMP versions 1 and 2c are subject to packet sniffing of the clear text community string from the network traffic, because they do not implement encryption.
- All versions of SNMP are subject to brute force and dictionary attacks for guessing the community strings, authentication strings, authentication keys, encryption strings, or encryption keys, because they do not implement a challenge-response handshake.
- Although SNMP works over TCP and other protocols, it is most commonly used over UDP that is connectionless and vulnerable to IP spoofing attacks. Thus, all versions are subject to bypassing device access lists that might have been implemented to restrict SNMP access, though SNMPv3's other security mechanisms should prevent a successful attack.
- SNMP's powerful configuration (write) capabilities are not being fully utilized by many vendors, partly because of a lack of security in SNMP versions before SNMPv3 and partly because many devices simply are not capable

of being configured via individual MIB object changes.

- SNMP tops the list of the SANS Institute's Common Default Configuration Issues with the issue of default SNMP community strings set to 'public' and 'private' and was number ten on the SANS Top 10 Most Critical Internet Security Threats<sup>[15]</sup> for the year 2000.

## Autodiscovery

SNMP by itself is simply a protocol for collecting and organizing information. Most toolsets implementing SNMP offer some form of discovery mechanism, a standardized collection of data common to most platforms and devices, to get a new user or implementor started. One of these features is often a form of automatic discovery, where new devices discovered in the network are polled automatically. For SNMPv1 and SNMPv2c, this presents a security risk, in that your SNMP read communities will be broadcast in cleartext to the target device. While security requirements and risk profiles vary from organization to organization, care should be taken when using a feature like this, with special regard to common environments such as mixed-tenant datacenters, server hosting and colocation facilities, and similar environments.

## RFC references

- RFC 1155 (STD 16) — *Structure and Identification of Management Information for the TCP/IP-based Internets*
- RFC 1156 (Historic) — *Management Information Base for Network Management of TCP/IP-based internets*
- RFC 1157 (Historic) — *A Simple Network Management Protocol (SNMP)*
- RFC 1213 (STD 17) — *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*
- RFC 1452 (Informational) — *Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework* (Obsoleted by RFC 1908)
- RFC 1901 (Experimental) — *Introduction to Community-based SNMPv2*
- RFC 1902 (Draft Standard) — *Structure of Management Information for SNMPv2* (Obsoleted by RFC 2578)
- RFC 1908 (Standards Track) — *Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework*
- RFC 2570 (Informational) — *Introduction to Version 3 of the Internet-standard Network Management Framework* (Obsoleted by RFC 3410)
- RFC 2578 (STD 58) — *Structure of Management Information Version 2 (SMIV2)*
- RFC 3410 (Informational) — *Introduction and Applicability Statements for Internet Standard Management Framework*
- STD 62
  - RFC 3411 — *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*
  - RFC 3412 — *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*
  - RFC 3413 — *Simple Network Management Protocol (SNMP) Applications*
  - RFC 3414 — *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
  - RFC 3415 — *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*
  - RFC 3416 — *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*
  - RFC 3417 — *Transport Mappings for the Simple Network Management Protocol (SNMP)*
  - RFC 3418 — *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*
- RFC 3430 (Experimental) — *Simple Network Management Protocol (SNMP) over Transmission Control Protocol (TCP) Transport Mapping*

- RFC 3584 (BCP 74) — *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*
- RFC 3826 (Proposed) — *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*
- RFC 5343 (Proposed) — *Simple Network Management Protocol (SNMP) Context EngineID Discovery*
- RFC 5590 (Draft) — *Transport Subsystem for the Simple Network Management Protocol (SNMP)*
- RFC 5591 (Draft) — *Transport Security Model for the Simple Network Management Protocol (SNMP)*
- RFC 5592 (Proposed) — *Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)*
- RFC 5608 (Proposed) — *Remote Authentication Dial-In User Service (RADIUS) Usage for Simple Network Management Protocol (SNMP) Transport Models.*
- RFC 6353 (Draft) — *Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)*

## References

- [1] Douglas R. Mauro & Kevin J. Schmidt. (2001). *Essential SNMP* (1st ed.). Sebastopol, CA: O'Reilly & Associates.
- [2] RFC 3411 — An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- [3] RFC 6353 Section 10
- [4] Douglas R. Mauro; Kevin J. Schmidt (July 2001), *Essential SNMP* ([http://docstore.mik.ua/orelly/networking\\_2ndEd/snmp/ch02\\_06.htm](http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_06.htm)), O'Reilly, ISBN 0-596-00020-0, , "Finally, SNMPv2 provides an inform mechanism, which allows for manager-to-manager communication."
- [5] *SNMP Inform Requests* ([http://www.cisco.com/en/US/docs/ios/11\\_3/feature/guide/snmpinfm.html](http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/snmpinfm.html)), Cisco, , retrieved 2011-12-09
- [6] "Security in SNMPv3 versus SNMPv1 or v2c" ([http://www.aethis.com/solutions/snmp\\_research/snmpv3\\_vs\\_wp.pdf](http://www.aethis.com/solutions/snmp_research/snmpv3_vs_wp.pdf)). . Retrieved 2010-11-29.
- [7] In This Issue: SNMP Version 3 (<http://www.simple-times.org/pub/simple-times/issues/5-1.html>) The Simple Times (<http://www.simple-times.org/>) ISSN 1060-6080
- [8] David Zeltserman (1999). *A Practical Guide to SNMPv3 and Network Management*. Upper Saddle River, NJ: Prentice Hall PTR.
- [9] "SNMPv3" (<http://www.webcitation.org/60I4lHgQR>). Cisco Systems. Archived from the original ([http://www.cisco.com/en/US/docs/ios/12\\_0t/12\\_0t3/feature/guide/Snmp3.html](http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html)) on 2011-07-19. .
- [10] "SNMP Version 3" (<http://www.ibr.cs.tu-bs.de/projects/snmpv3/>). Institute of Operating Systems and Computer Networks. . Retrieved 2010-05-07.
- [11] RFC Editor (<http://www.rfc-editor.org/categories/rfc-standard.html>) List of current Internet Standards (STDs)
- [12] RFC Editor (<http://www.rfc-editor.org/categories/rfc-historic.html>) List of HISTORIC RFCs
- [13] RFC 3584 "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework"
- [14] "SNMP Research presentations in favor of standards-based management over proprietary CLIs" (<http://www snmp com/conferences/>). SNMP Research. . Retrieved 2010-10-12.
- [15] <http://www.sans.org/top20/2000/>

## External links

- SNMP Portal (<http://www.snmplink.org/>)
- SNMP Programming starting point and reference (<http://www.cuddletech.com/articles/snmp/>)
- SNMP products and technical articles (<http://www.snmptools.net>)
- Cisco's description of SNMP and how to use in their products ([http://www.cisco.com/en/US/docs/ios/12\\_0t/12\\_0t3/feature/guide/Snmp3.html](http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html))
- SNMP: Simple? Network Management Protocol (<http://www.rane.com/note161.html>)
- Search engine for MIB files (<http://www.mibdepot.com/index.shtml>)
- Emnico SNMP MIB Library: A collection of SNMP MIBs (<http://www.emnico.com/mib>)
- SNMP v1, v2, and v3 Message Protocol Handy Reference (pdf) (created from an older set of RFCs) ([http://www.infrax.com/fr/network\\_protocols/snmp\\_protocol\\_reference.pdf](http://www.infrax.com/fr/network_protocols/snmp_protocol_reference.pdf))

# Internet Protocol Suite

The **Internet protocol suite** is the set of communications protocols used for the Internet and similar networks, and generally the most popular protocol stack for wide area networks. It is commonly known as **TCP/IP**, because of its most important protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP), which were the first networking protocols defined in this standard. It is occasionally known as the **DoD model** due to the foundational influence of the ARPANET in the 1970s (operated by DARPA, an agency of the United States Department of Defense).

TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. It has four abstraction layers, each with its own protocols.<sup>[1][2]</sup> From lowest to highest, the layers are:

1. The link layer (commonly Ethernet) contains communication technologies for a local network.
2. The internet layer (IP) connects local networks, thus establishing internetworking.
3. The transport layer (TCP) handles host-to-host communication.
4. The application layer (for example HTTP) contains all protocols for specific data communications services on a process-to-process level (for example how a web browser communicates with a web server).

The TCP/IP model and related protocols are maintained by the Internet Engineering Task Force (IETF).

## History

### Early research

The Internet protocol suite resulted from research and development conducted by the Defense Advanced Research Projects Agency (DARPA) in the early 1970s. After initiating the pioneering ARPANET in 1969, DARPA started work on a number of other data transmission technologies. In 1972, Robert E. Kahn joined the DARPA Information Processing Technology Office, where he worked on both satellite packet networks and ground-based radio packet networks, and recognized the value of being able to communicate across both. In the spring of 1973, Vinton Cerf, the developer of the existing ARPANET Network Control Program (NCP) protocol, joined Kahn to work on open-architecture interconnection models with the goal of designing the next protocol generation for the ARPANET.

By the summer of 1973, Kahn and Cerf had worked out a fundamental reformulation, where the differences between network protocols were hidden by using a common internetwork protocol, and, instead of the network being responsible for reliability, as in the ARPANET, the hosts became responsible. Cerf credits Hubert Zimmerman and Louis Pouzin, designer of the CYCLADES network, with important influences on this design.

The network's design included the recognition it should provide only the functions of efficiently transmitting and routing traffic between end nodes and that all other intelligence should be located at the edge of the network, in the end nodes. Using a simple design, it became possible to connect almost any network to the ARPANET, irrespective of their local characteristics, thereby solving Kahn's initial problem. One popular expression is that TCP/IP, the

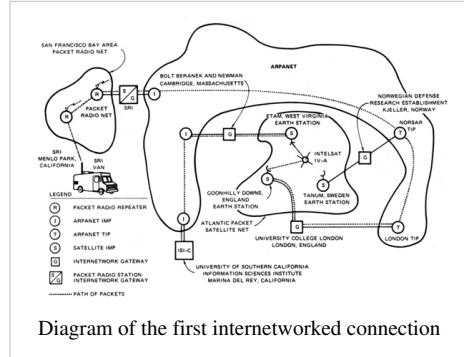


Diagram of the first internetworked connection



A Stanford Research Institute packet radio van,  
site of the first three-way internetworked  
transmission.

eventual product of Cerf and Kahn's work, will run over "*two tin cans and a string.*" As a joke, the IP over Avian Carriers formal protocol specification was created and successfully tested.

A computer called a router is provided with an interface to each network. It forwards packets back and forth between them.<sup>[3]</sup> Originally a router was called *gateway*, but the term was changed to avoid confusion with other types of gateways.

## Specification

From 1973 to 1974, Cerf's networking research group at Stanford worked out details of the idea, resulting in the first TCP specification.<sup>[4]</sup> A significant technical influence was the early networking work at Xerox PARC, which produced the PARC Universal Packet protocol suite, much of which existed around that time.

DARPA then contracted with BBN Technologies, Stanford University, and the University College London to develop operational versions of the protocol on different hardware platforms. Four versions were developed: TCP v1, TCP v2, TCP v3 and IP v3, and TCP/IP v4. The last protocol is still in use today.

In 1975, a two-network TCP/IP communications test was performed between Stanford and University College London (UCL). In November, 1977, a three-network TCP/IP test was conducted between sites in the US, the UK, and Norway. Several other TCP/IP prototypes were developed at multiple research centers between 1978 and 1983. The migration of the ARPANET to TCP/IP was officially completed on flag day January 1, 1983, when the new protocols were permanently activated.<sup>[5]</sup>

## Adoption

In March 1982, the US Department of Defense declared TCP/IP as the standard for all military computer networking.<sup>[6]</sup> In 1985, the Internet Architecture Board held a three-day workshop on TCP/IP for the computer industry, attended by 250 vendor representatives, promoting the protocol and leading to its increasing commercial use.

In 1985 the first Interop conference was held, focusing on network interoperability via further adoption of TCP/IP. It was founded by Dan Lynch, an early Internet activist. From the beginning, it was attended by large corporations, such as IBM and DEC. Interoperability conferences have been held every year since then. Every year from 1985 through 1993, the number of attendees tripled.

IBM, ATT and DEC were the first major corporations to adopt TCP/IP, despite having competing internal protocols (SNA, XNS, etc.). In IBM, from 1984, Barry Appelman's group did TCP/IP development. (Appelman later moved to AOL to be the head of all its development efforts.) They navigated the corporate politics to get a stream of TCP/IP products for various IBM systems, including MVS, VM, and OS/2. At the same time, several smaller companies began offering TCP/IP stacks for DOS and MS Windows, such as the company FTP Software, and the Wollongong Group.<sup>[7]</sup> The first VM/CMS TCP/IP stack came from the University of Wisconsin.<sup>[8]</sup>

Back then, most of these TCP/IP stacks were written single-handedly by a few talented programmers. For example, John Romkey of FTP Software was the author of the MIT PC/IP package.<sup>[9]</sup> John Romkey's PC/IP implementation was the first IBM PC TCP/IP stack. Jay Elinsky and Oleg Vishnepolsky of IBM Research wrote TCP/IP stacks for VM/CMS and OS/2, respectively.<sup>[10]</sup>

The spread of TCP/IP was fueled further in June 1989, when AT&T agreed to put into the public domain the TCP/IP code developed for UNIX. Various vendors, including IBM, included this code in their own TCP/IP stacks. Many companies sold TCP/IP stacks for Windows until Microsoft released its own TCP/IP stack in Windows 95. This event was a little late in the evolution of the Internet, but it cemented TCP/IP's dominance over other protocols, which eventually disappeared. These protocols included IBM's SNA, OSI, Microsoft's native NetBIOS, and Xerox' XNS.

## Key architectural principles

An early architectural document, RFC 1122, emphasizes architectural principles over layering.<sup>[11]</sup>

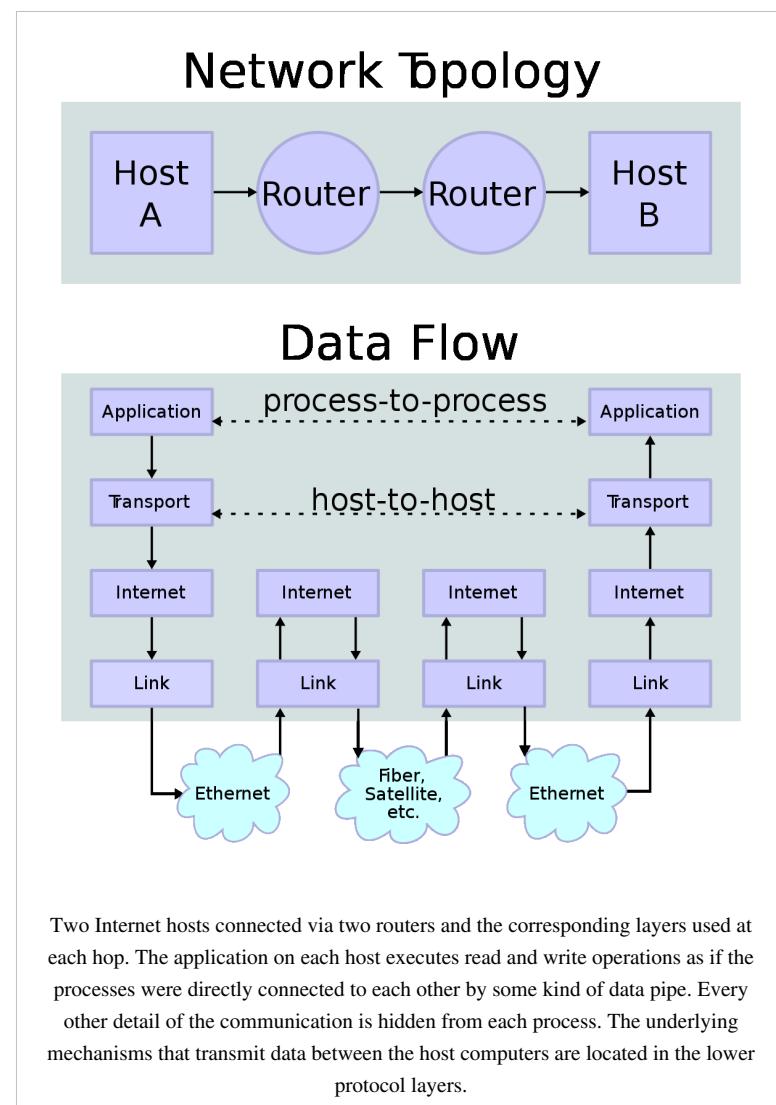
- End-to-end principle: This principle has evolved over time. Its original expression put the maintenance of state and overall intelligence at the edges, and assumed the Internet that connected the edges retained no state and concentrated on speed and simplicity. Real-world needs for firewalls, network address translators, web content caches and the like have forced changes in this principle.<sup>[12]</sup>
- Robustness Principle: "In general, an implementation must be conservative in its sending behavior, and liberal in its receiving behavior. That is, it must be careful to send well-formed datagrams, but must accept any datagram that it can interpret (e.g., not object to technical errors where the meaning is still clear)." <sup>[13]</sup> "The second part of the principle is almost as important: software on other hosts may contain deficiencies that make it unwise to exploit legal but obscure protocol features."<sup>[14]</sup>

## Layers in the Internet protocol suite

The Internet protocol suite uses encapsulation to provide abstraction of protocols and services. Encapsulation is usually aligned with the division of the protocol suite into layers of general functionality. In general, an application (the highest level of the model) uses a set of protocols to send its data down the layers, being further encapsulated at each level.

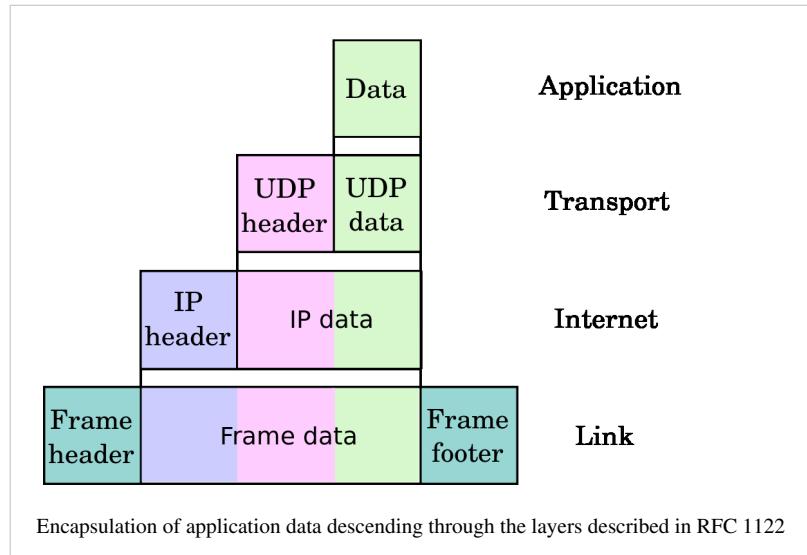
The "layers" of the protocol suite near the top are logically closer to the user application, while those near the bottom are logically closer to the physical transmission of the data. Viewing layers as providing or consuming a service is a method of abstraction to isolate upper layer protocols from the nitty-gritty detail of transmitting bits over, for example, Ethernet and collision detection, while the lower layers avoid having to know the details of each and every application and its protocol.

Even when the layers are examined, the assorted architectural documents—there is no single architectural model such as ISO 7498, the Open Systems Interconnection (OSI) model—have fewer and



less

rigidly defined layers than the OSI model, and thus provide an easier fit for real-world protocols. In point of fact, one frequently referenced document, RFC 1958, does not contain a stack of layers. The lack of emphasis on layering is a strong difference between the IETF and OSI approaches. It only refers to the existence of the "internetworking layer" and generally to "upper layers"; this document was intended as a 1996 "snapshot" of the architecture: "The Internet and its architecture have grown in evolutionary fashion from modest beginnings, rather than from a Grand Plan. While this process of evolution is one of the main reasons for the technology's success, it nevertheless seems useful to record a snapshot of the current principles of the Internet architecture."



Encapsulation of application data descending through the layers described in RFC 1122

RFC 1122, entitled *Host Requirements*, is structured in paragraphs referring to layers, but the document refers to many other architectural principles not emphasizing layering. It loosely defines a four-layer model, with the layers having names, not numbers, as follows:

- Application layer (process-to-process): This is the scope within which applications create user data and communicate this data to other processes or applications on another or the same host. The communications partners are often called *peers*. This is where the "higher level" protocols such as SMTP, FTP, SSH, HTTP, etc. operate.
- Transport layer (host-to-host): The transport layer constitutes the networking regime between two network hosts, either on the local network or on remote networks separated by routers. The transport layer provides a uniform networking interface that hides the actual topology (layout) of the underlying network connections. This is where flow-control, error-correction, and connection protocols exist, such as TCP. This layer deals with opening and maintaining connections between Internet hosts.
- Internet layer (internetworking): The internet layer has the task of exchanging datagrams across network boundaries. It is therefore also referred to as the layer that establishes internetworking, indeed, it defines and establishes the Internet. This layer defines the addressing and routing structures used for the TCP/IP protocol suite. The primary protocol in this scope is the Internet Protocol, which defines IP addresses. Its function in routing is to transport datagrams to the next IP router that has the connectivity to a network closer to the final data destination.
- Link layer: This layer defines the networking methods within the scope of the local network link on which hosts communicate without intervening routers. This layer describes the protocols used to describe the local network topology and the interfaces needed to affect transmission of Internet layer datagrams to next-neighbor hosts. (cf. the OSI data link layer).

The Internet protocol suite and the layered protocol stack design were in use before the OSI model was established. Since then, the TCP/IP model has been compared with the OSI model in books and classrooms, which often results in confusion because the two models use different assumptions, including about the relative importance of strict layering.

This abstraction also allows upper layers to provide services that the lower layers cannot, or choose not, to provide. Again, the original OSI model was extended to include connectionless services (OSIRM CL).<sup>[15]</sup> For example, IP is

not designed to be reliable and is a best effort delivery protocol. This means that all transport layer implementations must choose whether or not to provide reliability and to what degree. UDP provides data integrity (via a checksum) but does not guarantee delivery; TCP provides both data integrity and delivery guarantee (by retransmitting until the receiver acknowledges the reception of the packet).

This model lacks the formalism of the OSI model and associated documents, but the IETF does not use a formal model and does not consider this a limitation, as in the comment by David D. Clark, "We reject: kings, presidents and voting. We believe in: rough consensus and running code." Criticisms of this model, which have been made with respect to the OSI model, often do not consider ISO's later extensions to that model.

1. For multiaccess links with their own addressing systems (e.g. Ethernet) an address mapping protocol is needed. Such protocols can be considered to be below IP but above the existing link system. While the IETF does not use the terminology, this is a subnetwork dependent convergence facility according to an extension to the OSI model, the internal organization of the network layer (IONL).<sup>[16]</sup>
2. ICMP & IGMP operate on top of IP but do not transport data like UDP or TCP. Again, this functionality exists as layer management extensions to the OSI model, in its *Management Framework* (OSIRM MF)<sup>[17]</sup>
3. The SSL/TLS library operates above the transport layer (uses TCP) but below application protocols. Again, there was no intention, on the part of the designers of these protocols, to comply with OSI architecture.
4. The link is treated like a black box here. This is fine for discussing IP (since the whole point of IP is it will run over virtually anything). The IETF explicitly does not intend to discuss transmission systems, which is a less academic but practical alternative to the OSI model.

The following is a description of each layer in the TCP/IP networking model starting from the lowest level.

## Link layer

The link layer is the networking scope of the local network connection to which a host is attached. This regime is called the *link* in Internet literature. This is the lowest component layer of the Internet protocols, as TCP/IP is designed to be hardware independent. As a result TCP/IP is able to be implemented on top of virtually any hardware networking technology.

The link layer is used to move packets between the Internet layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets. These will perform data link functions such as adding a packet header to prepare it for transmission, then actually transmit the frame over a physical medium. The TCP/IP model includes specifications of translating the network addressing methods used in the Internet Protocol to data link addressing, such as Media Access Control (MAC), however all other aspects below that level are implicitly assumed to exist in the link layer, but are not explicitly defined.

This is also the layer where packets may be selected to be sent over a virtual private network or other networking tunnel. In this scenario, the link layer data may be considered application data which traverses another instantiation of the IP stack for transmission or reception over another IP connection. Such a connection, or virtual link, may be established with a transport protocol or even an application scope protocol that serves as a tunnel in the link layer of the protocol stack. Thus, the TCP/IP model does not dictate a strict hierarchical encapsulation sequence.

## Internet layer

The internet layer has the responsibility of sending packets across potentially multiple networks. Internetworking requires sending data from the source network to the destination network. This process is called routing.<sup>[18]</sup>

In the Internet protocol suite, the Internet Protocol performs two basic functions:

- *Host addressing and identification:* This is accomplished with a hierarchical addressing system (see IP address).
- *Packet routing:* This is the basic task of sending packets of data (datagrams) from source to destination by sending them to the next network node (router) closer to the final destination.

The internet layer is not only agnostic of application data structures as the transport layer, but it also does not distinguish between operation of the various transport layer protocols. So, IP can carry data for a variety of different upper layer protocols. These protocols are each identified by a unique protocol number: for example, Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP) are protocols 1 and 2, respectively.

Some of the protocols carried by IP, such as ICMP (used to transmit diagnostic information about IP transmission) and IGMP (used to manage IP Multicast data) are layered on top of IP but perform internetworking functions. This illustrates the differences in the architecture of the TCP/IP stack of the Internet and the OSI model.

The internet layer only provides an unreliable datagram transmission facility between hosts located on potentially different IP networks by forwarding the transport layer datagrams to an appropriate next-hop router for further relaying to its destination. With this functionality, the internet layer makes possible internetworking, the interworking of different IP networks, and it essentially establishes the Internet. The Internet Protocol is the principal component of the internet layer, and it defines two addressing systems to identify network hosts computers, and to locate them on the network. The original address system of the ARPANET and its successor, the Internet, is Internet Protocol version 4 (IPv4). It uses a 32-bit IP address and is therefore capable of identifying approximately four billion hosts. This limitation was eliminated by the standardization of Internet Protocol version 6 (IPv6) in 1998, and beginning production implementations in approximately 2006.

## Transport layer

The transport layer establishes host-to-host connectivity, meaning it handles the details of data transmission that are independent of the structure of user data and the logistics of exchanging information for any particular specific purpose. Its responsibility includes end-to-end message transfer independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers). End to end message transmission or connecting applications at the transport layer can be categorized as either connection-oriented, implemented in TCP, or connectionless, implemented in UDP.

The transport layer can be thought of as a transport mechanism, e.g., a vehicle with the responsibility to make sure that its contents (passengers/goods) reach their destination safely and soundly, unless another protocol layer is responsible for safe delivery. The layer simply establishes a basic data channel that an application uses in its task-specific data exchange.

For this purpose the layer establishes the concept of the port, a numbered logical construct allocated specifically for each of the communication channels an application needs. For many types of services, these port numbers have been standardized so that client computers may address specific services of a server computer without the involvement of service announcements or directory services.

Since IP provides only a best effort delivery, the transport layer is the first layer of the TCP/IP stack to offer reliability. IP can run over a reliable data link protocol such as the High-Level Data Link Control (HDLC).

For example, the TCP is a connection-oriented protocol that addresses numerous reliability issues to provide a reliable byte stream:

- data arrives in-order

- data has minimal error (i.e. correctness)
- duplicate data is discarded
- lost/discarded packets are resent
- includes traffic congestion control

The newer Stream Control Transmission Protocol (SCTP) is also a reliable, connection-oriented transport mechanism. It is message-stream-oriented — not byte-stream-oriented like TCP — and provides multiple streams multiplexed over a single connection. It also provides multi-homing support, in which a connection end can be represented by multiple IP addresses (representing multiple physical interfaces), such that if one fails, the connection is not interrupted. It was developed initially for telephony applications (to transport SS7 over IP), but can also be used for other applications.

User Datagram Protocol is a connectionless datagram protocol. Like IP, it is a best effort, "unreliable" protocol. Reliability is addressed through error detection using a weak checksum algorithm. UDP is typically used for applications such as streaming media (audio, video, Voice over IP etc.) where on-time arrival is more important than reliability, or for simple query/response applications like DNS lookups, where the overhead of setting up a reliable connection is disproportionately large. Real-time Transport Protocol (RTP) is a datagram protocol that is designed for real-time data such as streaming audio and video.

The applications at any given network address are distinguished by their TCP or UDP port. By convention certain *well known ports* are associated with specific applications. (*See List of TCP and UDP port numbers.*)

## Application layer

The application layer contains the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP).<sup>[19]</sup> Data coded according to application layer protocols are then encapsulated into one or (occasionally) more transport layer protocols (such as TCP or UDP), which in turn use lower layer protocols to effect actual data transfer.

Since the IP stack defines no layers between the application and transport layers, the application layer must include any protocols that act like the OSI's presentation and session layer protocols. This is usually done through libraries.

Application layer protocols generally treat the transport layer (and lower) protocols as black boxes which provide a stable network connection across which to communicate, although the applications are usually aware of key qualities of the transport layer connection such as the end point IP addresses and port numbers. As noted above, layers are not necessarily clearly defined in the Internet protocol suite. Application layer protocols are most often associated with client–server applications, and the commoner servers have specific ports assigned to them by the IANA: HTTP has port 80; Telnet has port 23; etc. Clients, on the other hand, tend to use ephemeral ports, i.e. port numbers assigned at random from a range set aside for the purpose.

Transport and lower level layers are largely unconcerned with the specifics of application layer protocols. Routers and switches do not typically "look inside" the encapsulated traffic to see what kind of application protocol it represents, rather they just provide a conduit for it. However, some firewall and bandwidth throttling applications do try to determine what's inside, as with the Resource Reservation Protocol (RSVP). It's also sometimes necessary for Network Address Translation (NAT) facilities to take account of the needs of particular application layer protocols. (NAT allows hosts on private networks to communicate with the outside world via a single visible IP address using port forwarding, and is an almost ubiquitous feature of modern domestic broadband routers).

## Layer names and number of layers in the literature

The following table shows various networking models. The number of layers varies between three and seven.

Kurose, <sup>[20]</sup> Forouzan <sup>[21]</sup>	Comer, <sup>[22]</sup> Kozierok <sup>[23]</sup>	Stallings <sup>[24]</sup>	Tanenbaum <sup>[25]</sup>	RFC 1122, Internet STD 3 (1989)	Cisco Academy <sup>[26]</sup>	Mike Padlipsky's 1982 "Arpanet Reference Model" (RFC 871)	OSI model
Five layers	Four+one layers	Five layers	Five layers	Four layers	Four layers	Three layers	Seven layers
"Five-layer Internet model" or "TCP/IP protocol suite"	"TCP/IP 5-layer reference model"	"TCP/IP model"	"TCP/IP 5-layer reference model"	"Internet model"	"Internet model"	"Arpanet reference model"	OSI model
Application	Application	Application	Application	Application	Application	Application/Process	Application
							Presentation
							Session
Transport	Transport	Host-to-host or transport	Transport	Transport	Transport	Host-to-host	Transport
Network	Internet	Internet	Internet	Internet	Internetwork		Network
Data link	Data link (Network interface)	Network access	Data link	Link	Network interface	Network interface	Data link
Physical	(Hardware)	Physical	Physical				Physical

Some of the networking models are from textbooks, which are secondary sources that may contravene the intent of RFC 1122 and other IETF primary sources.<sup>[27]</sup>

## OSI and TCP/IP layering differences

The three top layers in the OSI model—the application layer, the presentation layer and the session layer—are not distinguished separately in the TCP/IP model where it is just the application layer. While some pure OSI protocol applications, such as X.400, also combined them, there is no requirement that a TCP/IP protocol stack must impose monolithic architecture above the transport layer. For example, the NFS application protocol runs over the eXternal Data Representation (XDR) presentation protocol, which, in turn, runs over a protocol called Remote Procedure Call (RPC). RPC provides reliable record transmission, so it can run safely over the best-effort UDP transport.

Different authors have interpreted the RFCs differently, about whether the link layer (and the TCP/IP model) covers OSI model layer 1 (physical layer) issues, or if a hardware layer is assumed below the link layer.

Several authors have attempted to incorporate the OSI model's layers 1 and 2 into the TCP/IP model, since these are commonly referred to in modern standards (for example, by IEEE and ITU). This often results in a model with five layers, where the link layer or network access layer is split into the OSI model's layers 1 and 2.

The session layer roughly corresponds to the Telnet virtual terminal functionality, which is part of text based protocols such as the HTTP and SMTP TCP/IP model application layer protocols. It also corresponds to TCP and UDP port numbering, which is considered as part of the transport layer in the TCP/IP model. Some functions that would have been performed by an OSI presentation layer are realized at the Internet application layer using the MIME standard, which is used in application layer protocols such as HTTP and SMTP.

The IETF protocol development effort is not concerned with strict layering. Some of its protocols may not fit cleanly into the OSI model, although RFCs sometimes refer to it and often use the old OSI layer numbers. The IETF has repeatedly stated that Internet protocol and architecture development is not intended to be OSI-compliant. RFC 3439, addressing Internet architecture, contains a section entitled: "Layering Considered Harmful".<sup>[27]</sup>

Conflicts are apparent also in the original OSI model, ISO 7498, when not considering the annexes to this model (e.g., ISO 7498/4 Management Framework), or the ISO 8648 Internal Organization of the Network layer (IONL). When the IONL and Management Framework documents are considered, the ICMP and IGMP are neatly defined as layer management protocols for the network layer. In like manner, the IONL provides a structure for "subnetwork dependent convergence facilities" such as ARP and RARP.

IETF protocols can be encapsulated recursively, as demonstrated by tunneling protocols such as Generic Routing Encapsulation (GRE). GRE uses the same mechanism that OSI uses for tunneling at the network layer.

## Implementations

No specific hardware or software implementation is required by the protocols or the layered model, so there are many. Most computer operating systems in use today, including all consumer-targeted systems, include a TCP/IP implementation.

A minimally acceptable implementation includes the following protocols, listed from most essential to least essential: IP, ARP, ICMP, UDP, TCP and sometimes IGMP. In principle, it is possible to support only one transport protocol, such as UDP, but this is rarely done, because it limits usage of the whole implementation. IPv6, beyond its own version of ARP (NBP), ICMP (ICMPv6) and IGMP (IGMPv6), has some additional required functions, and often is accompanied by an integrated IPSec security layer. Other protocols could be easily added later (possibly being implemented entirely in userspace), such as DNS for resolving domain names to IP addresses, or DHCP for automatically configuring network interfaces.

Normally, application programmers are concerned only with interfaces in the application layer and often also in the transport layer, while the layers below are services provided by the TCP/IP stack in the operating system. Most IP implementations are accessible to programmers through sockets and APIs.

Unique implementations include Lightweight TCP/IP, an open source stack designed for embedded systems, and KA9Q NOS, a stack and associated protocols for amateur packet radio systems and personal computers connected via serial lines.

Microcontroller firmware in the network adapter typically handles link issues, supported by driver software in the operational system. Non-programmable analog and digital electronics are normally in charge of the physical components below the link layer, typically using an application-specific integrated circuit (ASIC) chipset for each network interface or other physical standard. High-performance routers are to a large extent based on fast non-programmable digital electronics, carrying out link level switching.

## References

- [1] RFC 1122, *Requirements for Internet Hosts – Communication Layers*, R. Braden (ed.), October 1989
- [2] RFC 1123, *Requirements for Internet Hosts – Application and Support*, R. Braden (ed.), October 1989
- [3] RFC 1812, *Requirements for IP Version 4 Routers*, F. Baker (June 1995)
- [4] RFC 675, *Specification of Internet Transmission Control Protocol*, V. Cerf et al. (December 1974)
- [5] Internet History (<http://www.livinginternet.com/i/ii.htm>)
- [6] Ronda Hauben. "From the ARPANET to the Internet" ([http://www.columbia.edu/~rh120/other/tcpdigest\\_paper.txt](http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt)). TCP Digest (UUCP). . Retrieved 2007-07-05.
- [7] Wollongong (<http://support.microsoft.com/kb/108007>)
- [8] A Short History of Internet Protocols at CERN (<http://www.weblab.isti.cnr.it/education/ssfs/lezioni/slides/archives/cern.htm>)
- [9] About | "romkey" (<http://www.romkey.com/about/>)
- [10] Barry Appelman
- [11] Architectural Principles of the Internet (<ftp://ftp.rfc-editor.org/in-notes/rfc1958.txt>), RFC 1958, B. Carpenter, June 1996
- [12] Rethinking the design of the Internet: The end to end arguments vs. the brave new world ([http://www.csdl.uoc.gr/~hy558/papers/Rethinking\\_2001.pdf](http://www.csdl.uoc.gr/~hy558/papers/Rethinking_2001.pdf)), Marjory S. Blumenthal, David D. Clark, August 2001
- [13] p.23 INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION September 1981 Jon Postel Editor (<http://www.ietf.org/rfc/rfc0791.txt?number=791>)

- [14] Requirements for Internet Hosts -- Communication Layers p.13 October 1989 R. Braden, Editor (<http://tools.ietf.org/html/rfc1122#page-12>)
- [15] [ OSI: Reference Model Addendum 1: Connectionless-mode Transmission,ISO7498/AD1],ISO7498/AD1, May 1986
- [16] "Information processing systems -- Open Systems Interconnection -- Internal organization of the Network Layer" ([http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=16011](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=16011)), ISO 8648:1988.
- [17] "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management framework" ([http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=14258](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=14258)), ISO 7498-4:1989.
- [18] IP Packet Structure (<http://www.comsci.us/datacom/ippacket.html>)
- [19] *TCP/IP Illustrated: the protocols* (<http://www.kohala.com/start/tcpipiv1.html>), ISBN 0-201-63346-9, W. Richard Stevens, February 1994
- [20] James F. Kurose, Keith W. Ross, Computer Networking: A Top-Down Approach, 2008, ISBN 0-321-49770-8 ([http://www.pearsonhighered.com/educator/academic/product/0,,0321497708,00+en-US\\_01DBC.html](http://www.pearsonhighered.com/educator/academic/product/0,,0321497708,00+en-US_01DBC.html))
- [21] Behrouz A. Forouzan, Data Communications and Networking, 2003 ([http://books.google.com/books?id=U3Gcf65Pu9IC&printsec=frontcover&q=forouzan+"computer+networks"&ei=RPZ9SOCvMofctAO02di0AQ&hl=en&sig=ACfU3U2Hh\\_n83pPtf5uCreCih0HnWvNcxg#PPA29,M1](http://books.google.com/books?id=U3Gcf65Pu9IC&printsec=frontcover&q=forouzan+"computer+networks"&ei=RPZ9SOCvMofctAO02di0AQ&hl=en&sig=ACfU3U2Hh_n83pPtf5uCreCih0HnWvNcxg#PPA29,M1))
- [22] Douglas E. Comer, Internetworking with TCP/IP: Principles, Protocols and Architecture, Pearson Prentice Hall 2005, ISBN 0-13-187671-6 ([http://books.google.com/books?id=jonyuTASbWAC&pg=PA155&hl=sv&source=gbts\\_toc\\_r&cad=0\\_0&sig=ACfU3U18gHAia1pU\\_Pxn-rhkCnH1v70M6Q#PPA161,M1](http://books.google.com/books?id=jonyuTASbWAC&pg=PA155&hl=sv&source=gbts_toc_r&cad=0_0&sig=ACfU3U18gHAia1pU_Pxn-rhkCnH1v70M6Q#PPA161,M1))
- [23] Charles M. Kozierok, "The TCP/IP Guide", No Starch Press 2005 (<http://books.google.com/books?id=Pm4RgYV2w4YC&pg=PA131&dq="TCP/IP+model+layers"&lr=&hl=sv&sig=ACfU3U3ofMwYAbZfGz1BmAXc2oNNFC2b8A#PPA129,M1>)
- [24] William Stallings, Data and Computer Communications, Prentice Hall 2006, ISBN 0-13-243310-9 ([http://books.google.com/books?id=c\\_AWmhkovR0C&pg=PA35&dq="internet+layer"+"network+access+layer"&ei=O99SI3EJo32sgOQpPThDw&hl=en&sig=ACfU3U38aXznzeAnQdbLcPFXfCgxAd4IFg](http://books.google.com/books?id=c_AWmhkovR0C&pg=PA35&dq="internet+layer"+"network+access+layer"&ei=O99SI3EJo32sgOQpPThDw&hl=en&sig=ACfU3U38aXznzeAnQdbLcPFXfCgxAd4IFg))
- [25] Andrew S. Tanenbaum, Computer Networks, Prentice Hall 2002, ISBN 0-13-066102-3 ([http://books.google.com/books?id=Pd-z64SJRBAC&pg=PA42&vq=internet+layer&dq=networks&hl=sv&source=gbts\\_search\\_s&sig=ACfU3U3DHAnIz0sOsd5NK4VXSrgNFYVAw#PPA42,M1](http://books.google.com/books?id=Pd-z64SJRBAC&pg=PA42&vq=internet+layer&dq=networks&hl=sv&source=gbts_search_s&sig=ACfU3U3DHAnIz0sOsd5NK4VXSrgNFYVAw#PPA42,M1))
- [26] Mark Dye, Mark A. Dye, Wendell, Network Fundamentals: CCNA Exploration Companion Guide, 2007, ISBN 1-58713-208-7
- [27] R. Bush; D. Meyer (December 2002), *Some Internet Architectural Guidelines and Philosophy* (<http://www.ietf.org/rfc/rfc3439.txt>), Internet Engineering Task Force, , retrieved 2012-01-07

## Further reading

- Douglas E. Comer. *Internetworking with TCP/IP - Principles, Protocols and Architecture*. ISBN 86-7991-142-9
- Joseph G. Davies and Thomas F. Lee. *Microsoft Windows Server 2003 TCP/IP Protocols and Services*. ISBN 0-7356-1291-9
- Forouzan, Behrouz A. (2003). *TCP/IP Protocol Suite* (2nd ed.). McGraw-Hill. ISBN 0-07-246060-1.
- Craig Hunt *TCP/IP Network Administration*. O'Reilly (1998) ISBN 1-56592-322-7
- Maufer, Thomas A. (1999). *IP Fundamentals*. Prentice Hall. ISBN 0-13-975483-0.
- Ian McLean. *Windows(R) 2000 TCP/IP Black Book*. ISBN 1-57610-687-X
- Ajit Mungale *Pro .NET 1.1 Network Programming*. ISBN 1-59059-345-6
- W. Richard Stevens. *TCP/IP Illustrated, Volume 1: The Protocols*. ISBN 0-201-63346-9
- W. Richard Stevens and Gary R. Wright. *TCP/IP Illustrated, Volume 2: The Implementation*. ISBN 0-201-63354-X
- W. Richard Stevens. *TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols*. ISBN 0-201-63495-3
- Andrew S. Tanenbaum. *Computer Networks*. ISBN 0-13-066102-3
- Clark, D. (1988). "The Design Philosophy of the DARPA Internet Protocols" (<http://www.cs.princeton.edu/~jrex/teaching/spring2005/reading/clark88.pdf>). *SIGCOMM '88 Symposium proceedings on Communications architectures and protocols* (ACM): 106–114. doi:10.1145/52324.52336. Retrieved 2011-10-16.

## External links

- Internet History (<http://www.livinginternet.com/i/ii.htm>)—Pages on Robert Kahn, Vinton Cerf, and TCP/IP (reviewed by Cerf and Kahn).
- RFC 675 (<http://www.ietf.org/rfc/rfc0675.txt>) - Specification of Internet Transmission Control Program, December 1974 Version
- TCP/IP State Transition Diagram ([http://www.night-ray.com/TCPIP\\_State\\_Transition\\_Diagram.pdf](http://www.night-ray.com/TCPIP_State_Transition_Diagram.pdf)) (PDF)
- RFC 1180 A TCP/IP Tutorial - from the Internet Engineering Task Force (January 1991)
- TCP/IP FAQ (<http://www.itprc.com/tcpipfaq/>)
- The TCP/IP Guide (<http://www.tcpipguide.com/free/>) - A comprehensive look at the protocols and the procedures/processes involved
- A Study of the ARPANET TCP/IP Digest ([http://www.columbia.edu/~rh120/other/tcdigest\\_paper.txt](http://www.columbia.edu/~rh120/other/tcdigest_paper.txt))
- TCP/IP Sequence Diagrams (<http://www.eventhelix.com/RealtimeMantra/Networking/>)
- The Internet in Practice (<http://www.searchandgo.com/articles/internet/internet-practice-4.php>)
- TCP/IP - Directory & Informational Resource (<http://softtechinfo.com/network/tcpip.html>)
- Daryl's TCP/IP Primer (<http://www.ipprimer.com/>) - Intro to TCP/IP LAN administration, conversational style
- Introduction to TCP/IP (<http://www.linux-tutorial.info/MContent-142>)
- TCP/IP commands from command prompt (<http://blog.webgk.com/2007/10/dns-tcpip-commands-from-command-prompt.html>)
- cIPS (<http://sourceforge.net/projects/cipsuite/>) — Robust TCP/IP stack for embedded devices without an Operating System

# Internet Control Message Protocol

---

The **Internet Control Message Protocol (ICMP)** is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.<sup>[1]</sup> It is assigned protocol number 1.<sup>[2]</sup>

ICMP<sup>[3]</sup> differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).

ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4. IPv6 has a similar protocol, ICMPv6.

## Technical details

The Internet Control Message Protocol is part of the Internet Protocol Suite, as defined in RFC 792. ICMP messages are typically used for diagnostic or control purposes or generated in response to errors in IP operations (as specified in RFC 1122). ICMP errors are directed to the source IP address of the originating packet.<sup>[1]</sup>

For example, every device (such as an intermediate router) forwarding an IP datagram first decrements the time to live (TTL) field in the IP header by one. If the resulting TTL is 0, the packet is discarded and an ICMP Time To Live exceeded in transit message is sent to the datagram's source address.

Although ICMP messages are contained within standard IP datagrams, ICMP messages are usually processed as a special case, distinguished from normal IP processing, rather than processed as a normal sub-protocol of IP. In many cases, it is necessary to inspect the contents of the ICMP message and deliver the appropriate error message to the application that generated the original IP packet, the one that prompted the sending of the ICMP message.

Many commonly used network utilities are based on ICMP messages. The tracert (traceroute), Pathping commands are implemented by transmitting UDP datagrams with specially set IP TTL header fields, and looking for ICMP Time to live exceeded in transit (above) and "Destination unreachable" messages generated in response. The related ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.

## ICMP segment structure

### Header

The ICMP header starts after the IPv4 header. All ICMP packets will have an 8-byte header and variable-sized data section. The first 4 bytes of the header will be consistent. The first byte is for the ICMP type. The second byte is for the ICMP code. The third and fourth bytes are a checksum of the entire ICMP message. The contents of the remaining 4 bytes of the header will vary based on the ICMP type and code.<sup>[1]</sup>

ICMP error messages contain a data section that includes the entire IP header plus the first 8 bytes of data from the IP datagram that caused the error message. The ICMP datagram is then encapsulated in a new IP datagram.<sup>[1]</sup>

Bits	0–7	8–15	16–23	24–31
<b>0</b>	Type	Code	Checksum	
<b>32</b>	Rest of Header			

- **Type** – ICMP type as specified below.
- **Code** – Subtype to the given type.
- **Checksum** – Error checking data. Calculated from the ICMP header+data, with value 0 for this field. The checksum algorithm is specified in RFC 1071<sup>[4]</sup>.
- **Rest of Header** – Four byte field. Will vary based on the ICMP type and code.

### List of permitted control messages (incomplete list)

Type	Code	Description
0 – Echo Reply <sup>[5]</sup>	0	Echo reply (used to ping)
1 and 2		<i>Reserved</i>

3 – Destination Unreachable <sup>[6]</sup>	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation required, and DF flag set
	5	Source route failed
	6	Destination network unknown
	7	Destination host unknown
	8	Source host isolated
	9	Network administratively prohibited
	10	Host administratively prohibited
	11	Network unreachable for TOS
	12	Host unreachable for TOS
	13	Communication administratively prohibited
	14	Host Precedence Violation
	15	Precedence cutoff in effect
4 – Source Quench	0	Source quench (congestion control)
5 – Redirect Message	0	Redirect Datagram for the Network
	1	Redirect Datagram for the Host
	2	Redirect Datagram for the TOS & network
	3	Redirect Datagram for the TOS & host
6		Alternate Host Address
7		<i>Reserved</i>
8 – Echo Request	0	Echo request (used to ping)
9 – Router Advertisement	0	Router Advertisement
10 – Router Solicitation	0	Router discovery/selection/solicitation
11 – Time Exceeded <sup>[7]</sup>	0	TTL expired in transit
	1	Fragment reassembly time exceeded
12 – Parameter Problem: Bad IP header	0	Pointer indicates the error
	1	Missing a required option
	2	Bad length
13 – Timestamp	0	Timestamp
14 – Timestamp Reply	0	Timestamp reply
15 – Information Request	0	Information Request
16 – Information Reply	0	Information Reply
17 – Address Mask Request	0	Address Mask Request
18 – Address Mask Reply	0	Address Mask Reply
19		<i>Reserved</i> for security
20 through 29		<i>Reserved</i> for robustness experiment

30 – Traceroute	0	Information Request
31		Datagram Conversion Error
32		Mobile Host Redirect
33		Where-Are-You (originally meant for IPv6)
34		Here-I-Am (originally meant for IPv6)
35		Mobile Registration Request
36		Mobile Registration Reply
37		Domain Name Request
38		Domain Name Reply
39		SKIP Algorithm Discovery Protocol, Simple Key-Management for Internet Protocol
40		Photuris, Security failures
41		ICMP for experimental mobility protocols such as Seamoby [RFC4065]
42 through 255		<i>Reserved</i>

(Sources: IANA ICMP Parameters <sup>[8]</sup> [9] and *Computer Networking – A Top-Down Approach* by Kurose and Ross)

//

## References

- [1] Forouzan, Behrouz A. (2007). *Data Communications And Networking* (Fourth ed.). Boston: McGraw-Hill. pp. 621–630.  
ISBN 0-07-296775-7.
- [2] "Protocol Numbers" (<http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml>). . Internet Assigned Numbers Authority. . Retrieved 2011-06-23.
- [3] Postel, J. (September 1981). *Internet Control Message Protocol* (<https://tools.ietf.org/html/rfc792>). IETF. RFC 792. .
- [4] <http://tools.ietf.org/html/rfc1071>
- [5] <http://tools.ietf.org/html/rfc792#page-14>
- [6] <http://tools.ietf.org/html/rfc792#page-4>
- [7] <http://tools.ietf.org/html/rfc792#page-6>
- [8] <http://www.iana.org/assignments/icmp-parameters>
- [9] [http://freebie.fatpipe.org/~mjb/Drawings/UDP\\_ICMP\\_Headers.png](http://freebie.fatpipe.org/~mjb/Drawings/UDP_ICMP_Headers.png)

## External links

- RFCs
  - RFC 792, *Internet Control Message Protocol*
  - RFC 1122, *Requirements for Internet Hosts – Communication Layers*
  - RFC 1716, *Towards Requirements for IP Router*
  - RFC 1812, *Requirements for IP Version 4 Routers*
- IANA ICMP parameters (<http://www.iana.org/assignments/icmp-parameters>)
- IANA protocol numbers (<http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml>)

# Internet Group Management Protocol

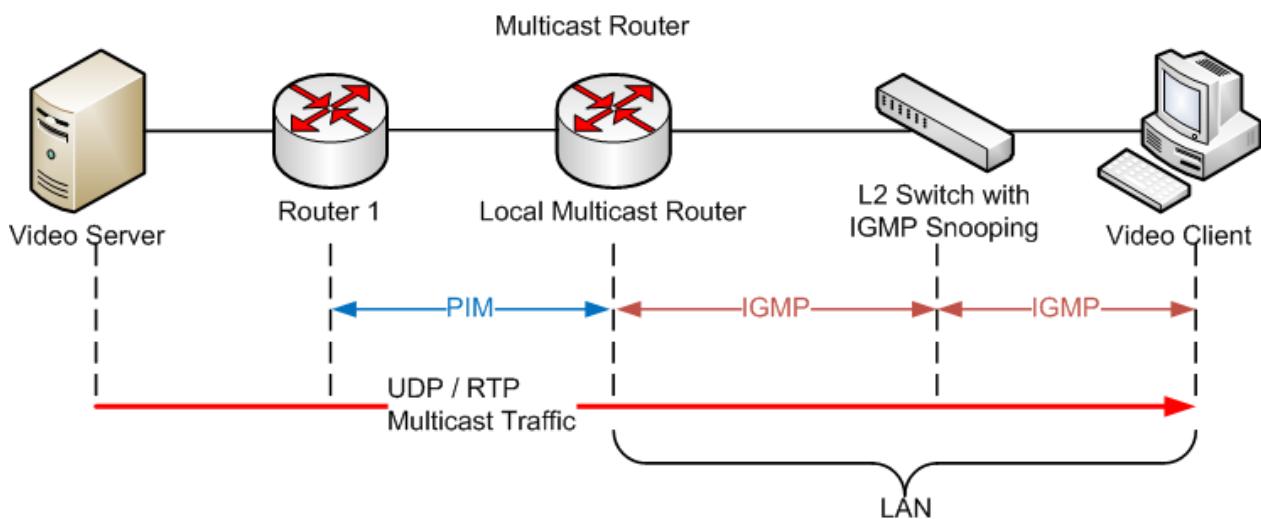
The **Internet Group Management Protocol (IGMP)** is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP is an integral part of the IP multicast specification. It is analogous to ICMP for unicast connections. IGMP can be used for online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

IGMP is used on IPv4 networks. Multicast management on IPv6 networks is handled by Multicast Listener Discovery (MLD) which uses ICMPv6 messaging in contrast to IGMP's bare IP encapsulation.

## Architecture

A network designed to deliver a multicast service using IGMP might use this basic architecture:



IGMP operates between the client computer and a local multicast router. Switches featuring IGMP snooping derive useful information by observing these IGMP transactions. Protocol Independent Multicast (PIM) is then used between the local and remote multicast routers, to direct multicast traffic from the multicast server to many multicast clients.

IGMP operates above the network layer, though it does not actually act as a transport protocol.<sup>[1]</sup>

## Standards

There are three versions of IGMP, as defined by Request for Comments (RFC) documents of the Internet Engineering Task Force (IETF). IGMPv1 is defined by RFC 1112, IGMPv2 is defined by RFC 2236 and IGMPv3 was initially defined by RFC 3376 and has been updated by RFC 4604 which defines both IGMPv3 and MLDv2. IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group. IGMPv3 improves over IGMPv2 mainly by adding the ability to listen to multicast originating from a set of source IP addresses only.<sup>[2]</sup>

## Host and router implementations

The IGMP protocol is implemented on a particular host and within a router. A host requests membership to a group through its local router while a router listens for these requests and periodically sends out subscription queries. The FreeBSD,<sup>[3]</sup> Linux<sup>[4]</sup> and Windows operating systems support IGMP at the host side.

For the server side implementation, the Linux case uses a daemon such as mrouted to act as an IGMP Linux router. There are also entire routing suites (such as XORP or Quagga), which turn an ordinary computer into a full-fledged multicast router.

## Security

IGMP is vulnerable to some attacks,<sup>[5][6][7][8]</sup> and firewalls commonly allow the user to disable it if not needed.

## IGMPv3 packet structure

IGMP messages are carried in bare IP packets with IP protocol number 2.<sup>[9]</sup> There is no transport layer used with IGMP messaging, similar to ICMP for example.

### Membership Query Message

Membership Queries are sent by multicast routers to determine which multicast addresses are of interest to systems attached to its network. Routers periodically send General Queries to refresh the group membership state for all systems on its network. Group-Specific Queries are used for determining the reception state for a particular multicast address. Group-and-Source-Specific Queries allow the router to determine if any systems desire reception of messages sent to a multicast group from a source address specified in a list of unicast addresses.

### IGMPv3 packet structure

bit offset	0–3	4	5–7	8–15	16–31
0	Type = 0x11			Max Resp Code	Checksum
32	Group Address				
64	Resv	S	QRV	QQIC	Number of Sources (N)
96	Source Address [1]				
128	Source Address [2]				
	...				
	Source Address [N]				

#### Max Resp Code

This field specifies the maximum time (in 1/10 second) allowed before sending a responding report. If the number is below 128, the value is used directly. If the value is 128 or more, it is interpreted as an exponent and mantissa.

#### Checksum

This is the 16-bit one's complement of the one's complement sum of the entire IGMP message.

#### Group Address

This is the multicast address being queried when sending a Group-Specific or Group-and-Source-Specific Query. The field is zeroed when sending a General Query.

#### Resv

This field is reserved. It should be zeroed when sent and ignored when received.

#### S (Suppress Router-side Processing) Flag

When this flag is set, it indicates to receiving routers that they are to suppress the normal timer updates.

#### QRV (Querier's Robustness Variable)

If this is non-zero, it contains the Robustness Variable value used by the sender of the Query. Routers should update their Robustness Variable to match the most recently received Query unless the value is zero.

#### QQIC (Querier's Query Interval Code)

This code is used for specify the Query Interval value (in seconds) used by the querier. If the number is below 128, the value is used directly. If the value is 128 or more, it is interpreted as an exponent and mantissa.

#### Number of Sources (N)

This field specifies the number of source addresses present in the Query. For General and Group-Specific Queries, this value is zero. For Group-and-Source-Specific Queries, this value is non-zero, but limited by the network's MTU.

#### Source Address [i]

The Source Address [i] fields are a vector of n IP unicast addresses, where n is the value in the Number of Sources (N) field.

## IGMPv2 packet structure

### IGMPv2 packet structure

+	Bits 0–7	8–15	16–31
0	Type	Max Resp Time	Checksum
32	Group Address		

Defined by RFC 2236 <sup>[10]</sup>

Where:

- Type is Membership Query (0x11), Membership Report (IGMPv1: 0x12, IGMPv2: 0x16), Leave Group (0x17)  
IGMPv3 adds type Membership Report (0x22)
- Max Resp Time specifies the time limit for the corresponding report. The field has a resolution of 100 milliseconds, the value is taken directly. This field is meaningful only in Membership Query (0x11); in other messages it is set to 0 and ignored by the receiver.

## Notes

- [1] "IGMP, Internet Group Management Protocol" (<http://www.networksorcery.com/enp/protocol/igmp.htm>). Network Sorcery.. Retrieved 2010-11-18.
- [2] "Internet Group Management Protocol Overview" (<http://www.javvin.com/protocolIGMP.html>). Javvin.. Retrieved 2010-11-18.
- [3] IGMPv3 was added to FreeBSD in version 8.0.
- [4] IGMPv3 was added in the Linux 2.5 kernel series.
- [5] Spoofed IGMP report denial of service (<http://www.securityfocus.com/bid/5020/info>) vulnerability.
- [6] Fragmented IGMP packet (<http://support.microsoft.com/default.aspx?scid=kb;en-us;238329&sd=tech>) may promote "Denial of Service" attack.
- [7] IGMP Security Problem Statement and Requirements ([http://www.securemulticast.org/GSEC/gsec3\\_ietf53\\_SecureIGMP1.pdf#search=%22igmp%20attacks%22](http://www.securemulticast.org/GSEC/gsec3_ietf53_SecureIGMP1.pdf#search=%22igmp%20attacks%22)).
- [8] Microsoft Security Bulletin MS06-007: Vulnerability in TCP/IP Could Allow Denial of Service (913446) (<http://www.microsoft.com/technet/security/Bulletin/MS06-007.mspx>).
- [9] RFC 3376 section 4

[10] <http://tools.ietf.org/html/rfc2236#section-2>

## References

### External links

- IPv4 Multicasting Tools and Settings on Microsoft TechNet (<http://technet2.microsoft.com/WindowsServer/en/Library/fe09af2c-3deb-4c6c-a79f-35c6953a8c9d1033.mspx>)
- Different version and details on IGMP (<http://www.commsdesign.com/article/printableArticle.jhtml?articleID=52200253>)

# Simple Mail Transfer Protocol

**Simple Mail Transfer Protocol (SMTP)** is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks. SMTP was first defined by RFC 821 (1982, eventually declared STD 10),<sup>[1]</sup> and last updated by RFC 5321 (2008)<sup>[2]</sup> which includes the extended SMTP (ESMTP) additions, and is the protocol in widespread use today. SMTP uses TCP port 25. The protocol for new submissions (MSA) is effectively the same as SMTP, but it uses port 587 instead. SMTP connections secured by SSL are known by the shorthand SMTPS, though SMTPS is not a protocol in its own right.

While electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically only use SMTP for sending messages to a mail server for relaying. For receiving messages, client applications usually use either the Post Office Protocol (POP) or the Internet Message Access Protocol (IMAP) or a proprietary system (such as Microsoft Exchange or Lotus Notes/Domino) to access their mail box accounts on a mail server.

## History

Various forms of one-to-one electronic messaging were used in the 1960s. People communicated with one another using systems developed for specific mainframe computers. As more computers were interconnected, especially in the US Government's ARPANET, standards were developed to allow users of different systems to e-mail one another. SMTP grew out of these standards developed during the 1970s.

SMTP can trace its roots to two implementations described in 1971, the Mail Box Protocol, which has been disputed to actually have been implemented,<sup>[3]</sup> but is discussed in RFC 196 and other RFCs, and the SNDMSG program, which, according to RFC 2235, Ray Tomlinson of BBN "invents" for TENEX computers the sending of mail across the ARPANET.<sup>[4][5][6]</sup> Fewer than 50 hosts were connected to the ARPANET at this time.<sup>[7]</sup>

Further implementations include FTP Mail<sup>[8]</sup> and Mail Protocol, both from 1973.<sup>[9]</sup> Development work continued throughout the 1970s, until the ARPANET converted into the modern Internet around 1980. Jon Postel then proposed a Mail Transfer Protocol in 1980 that began to remove the mail's reliance on FTP.<sup>[10]</sup> SMTP was published as RFC 788 in November 1981, also by Postel.

The SMTP standard was developed around the same time as Usenet, a one-to-many communication network with some similarities.

SMTP became widely used in the early 1980s. At the time, it was a complement to Unix to Unix Copy Program (UUCP) mail, which was better suited for handling e-mail transfers between machines that were intermittently connected. SMTP, on the other hand, works best when both the sending and receiving machines are connected to the network all the time. Both use a store and forward mechanism and are examples of push technology. Though Usenet's newsgroups are still propagated with UUCP between servers,<sup>[11]</sup> UUCP mail has virtually disappeared<sup>[12]</sup>

along with the "bang paths" it used as message routing headers.

The article about sender rewriting contains technical background info about the early SMTP history and source routing before RFC 1123.

Released with 4.1cBSD, right after RFC 788, Sendmail was one of the first (if not the first) mail transfer agents to implement SMTP.<sup>[13]</sup> Over time, as BSD Unix became the most popular operating system on the Internet, sendmail became the most common MTA.<sup>[14]</sup> Some other popular SMTP server programs include Postfix, qmail, Novell GroupWise, Exim, Novell NetMail, Microsoft Exchange Server, Sun Java System Messaging Server.

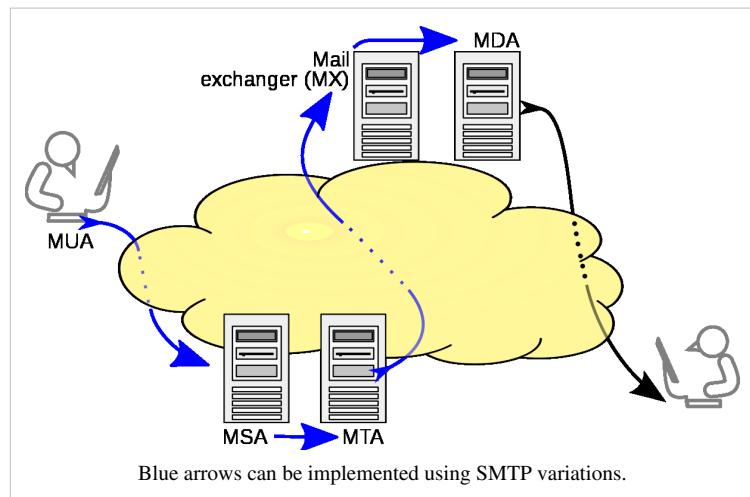
Message submission (RFC 2476) and SMTP-AUTH (RFC 2554) were introduced in 1998 and 1999, both describing new trends in e-mail delivery. Originally, SMTP servers were typically internal to an organization, receiving mail for the organization *from the outside*, and relaying messages from the organization *to the outside*. But as time went on, SMTP servers (Mail transfer agents), in practice, were expanding their roles to become message submission agents for Mail user agents, some of which were now relaying mail *from the outside* of an organization. (e.g. a company executive wishes to send e-mail while on a trip using the corporate SMTP server.) This issue, a consequence of the rapid expansion and popularity of the World Wide Web, meant that SMTP had to include specific rules and methods for relaying mail and authenticating users to prevent abuses such as relaying of unsolicited e-mail (spam).

As this protocol started out purely ASCII text-based, it did not deal well with binary files, or characters in many non-English languages. Standards such as Multipurpose Internet Mail Extensions (MIME) were developed to encode binary files for transfer through SMTP. Mail transfer agents (MTAs) developed after Sendmail also tended to be implemented 8-bit-clean, so that the alternate "just send eight" strategy could be used to transmit arbitrary text data (in any 8-bit ASCII-like character encoding) via SMTP. Mojibake was still a problem due to differing character set mappings between vendors, although the email addresses themselves still allowed only ASCII. 8-bit-clean MTAs today tend to support the 8BITMIME extension, permitting binary files to be transmitted almost as easily as plain text. Recently the SMTPUTF8 extension was created to support UTF-8 text, allowing international content and addresses in non-Latin scripts like Cyrillic or Chinese.

Many people contributed to the core SMTP specifications, among them Jon Postel, Eric Allman, Dave Crocker, Ned Freed, Randall Gellens, John Klensin, and Keith Moore.

## Mail processing model

Email is submitted by a mail client (MUA, mail user agent) to a mail server (MSA, mail submission agent) using SMTP on TCP port 587. Most mailbox providers still allow submission on traditional port 25. From there, the MSA delivers the mail to its mail transfer agent (MTA, mail transfer agent). Often, these two agents are just different instances of the same software launched with different options on the same machine. Local processing can be done either on a single machine, or split among various appliances; in the former case, involved processes can share files; in the latter case, SMTP is used to transfer the message internally, with each host configured to use the next appliance as a smart host. Each process is an MTA in its own right; that is, an SMTP server.



The boundary MTA has to locate the target host. It uses the Domain name system (DNS) to look up the mail exchanger record (MX record) for the recipient's domain (the part of the address on the right of @). The returned MX record contains the name of the target host. The MTA next connects to the exchange server as an SMTP client. (The article on MX record discusses many factors in determining which server the sending MTA connects to.)

Once the MX target accepts the incoming message, it hands it to a mail delivery agent (MDA) for local mail delivery. An MDA is able to save messages in the relevant mailbox format. Again, mail reception can be done using many computers or just one —the picture displays two nearby boxes in either case. An MDA may deliver messages directly to storage, or forward them over a network using SMTP, or any other means, including the Local Mail Transfer Protocol (LMTP), a derivative of SMTP designed for this purpose.

Once delivered to the local mail server, the mail is stored for batch retrieval by authenticated mail clients (MUAs). Mail is retrieved by end-user applications, called email clients, using Internet Message Access Protocol (IMAP), a protocol that both facilitates access to mail and manages stored mail, or the Post Office Protocol (POP) which typically uses the traditional mbox mail file format or a proprietary system such as Microsoft Exchange/Outlook or Lotus Notes/Domino. Webmail clients may use either method, but the retrieval protocol is often not a formal standard.

SMTP defines message *transport*, not the message *content*. Thus, it defines the mail *envelope* and its parameters, such as the envelope sender, but not the header or the body of the message itself. STD 10 and RFC 5321 define SMTP (the envelope), while STD 11 and RFC 5322 define the message (header and body), formally referred to as the Internet Message Format.

## Protocol overview

SMTP is a connection-oriented, text-based protocol in which a mail sender communicates with a mail receiver by issuing command strings and supplying necessary data over a reliable ordered data stream channel, typically a Transmission Control Protocol (TCP) connection. An *SMTP session* consists of commands originated by an SMTP client (the initiating agent, sender, or transmitter) and corresponding responses from the SMTP server (the listening agent, or receiver) so that the session is opened, and session parameters are exchanged. A session may include zero or more SMTP transactions. An *SMTP transaction* consists of three command/reply sequences (see example below.) They are:

1. **MAIL** command, to establish the return address, a.k.a. Return-Path, 5321.From, mfrom, or envelope sender. This is the address for bounce messages.
2. **RCPT** command, to establish a recipient of this message. This command can be issued multiple times, one for each recipient. These addresses are also part of the envelope.
3. **DATA** to send the *message text*. This is the content of the message, as opposed to its envelope. It consists of a *message header* and a *message body* separated by an empty line. DATA is actually a group of commands, and the server replies twice: once to the *DATA command* proper, to acknowledge that it is ready to receive the text, and the second time after the end-of-data sequence, to either accept or reject the entire message.

Besides the intermediate reply for DATA, each server's reply can be either positive (2xx reply codes) or negative. Negative replies can be permanent (5xx codes) or transient (4xx codes). A **reject** is a permanent failure by an SMTP server; in this case the SMTP client should send a bounce message. A **drop** is a positive response followed by message discard rather than delivery.

The initiating host, the SMTP client, can be either an end-user's email client, functionally identified as a mail user agent (MUA), or a relay server's mail transfer agent (MTA), that is an SMTP server acting as an SMTP client, in the relevant session, in order to relay mail. Fully capable SMTP servers maintain queues of messages for retrying message transmissions that resulted in transient failures.

A MUA knows the *outgoing mail* SMTP server from its configuration. An SMTP server acting as client, i.e. *relaying*, typically determines which SMTP server to connect to by looking up the MX (Mail eXchange) DNS resource record for each recipient's domain name. Conformant MTAs (not all) fall back to a simple A record in case no MX record can be found. Relaying servers can also be configured to use a smart host.

An SMTP server acting as client initiates a TCP connection to the server on the "well-known port" designated for SMTP: port 25. MUAs should use port 587 to connect to an MSA. The main difference between an MTA and an MSA is that SMTP Authentication is mandatory for the latter only.

## SMTP vs mail retrieval

SMTP is a delivery protocol only. It cannot *pull* messages from a remote server on demand. Other protocols, such as the Post Office Protocol (POP) and the Internet Message Access Protocol (IMAP) are specifically designed for retrieving messages and managing mail boxes. However, SMTP has a feature to initiate mail queue processing on a remote server so that the requesting system may receive any messages destined for it (see Remote Message Queue Starting below). POP and IMAP are preferred protocols when a user's personal computer is only intermittently powered up, or Internet connectivity is only transient and hosts cannot receive message during off-line periods.

## Remote Message Queue Starting

Remote Message Queue Starting is a feature of SMTP that permits a remote host to start processing of the mail queue on a server so it may receive messages destined to it by sending the TURN command. This feature however was deemed insecure<sup>[15]</sup> and was extended in RFC 1985 with the ETRN command which operates more securely using an authentication method based on Domain Name System information.

## On-Demand Mail Relay

**On-Demand Mail Relay (ODMR)** is an SMTP extension standardized in RFC 2645 that allows e-mail to be relayed to an authenticated recipient.

## Internationalization

Many users whose native script is not Latin based have had difficulty with the Latin email address requirement. Often this leads to meaningless, but easy to type, locale addresses.

RFC 6531 was created to solve that problem, providing internationalization features for SMTP, the SMTPUTF8 extension. RFC 6531 provides support for multi-byte and non-ASCII characters in email addresses, such as Pelé@live.com (simple diacritic), δοκιμή@παράδειγμα.δοκιμή, and 测试@测试.测试. Current support is limited, but there is strong interest in broad adoption of RFC 6531 and the related RFCs in countries like China that have a large user base where Latin (ASCII) is a foreign script.

## Outgoing mail SMTP server

An e-mail client needs to know the IP address of an SMTP server and this has to be given as part of its configuration (usually given as a DNS name). The server will deliver outgoing messages on behalf of the user.

### Outgoing mail server access restrictions

Server administrators need to impose some control on which clients can use the server. This enables them to deal with abuse, for example spam. Two solutions have been in common use:

- In the past, many systems imposed usage restrictions by the *location* of the client, only permitting usage by clients whose IP address is one that the server administrators control. Usage from any other client IP address is disallowed.
- Modern SMTP servers typically offer an alternative system that requires authentication of clients by credentials before allowing access.

#### Restricting access by location

Under this system, an *ISP's* SMTP server will not allow access by users who are 'outside the ISP's network'. More precisely, the server may only allow access to users with an IP address provided by the ISP, which is equivalent to requiring that they are connected to the Internet using that same ISP. A mobile user may often be on a network other than that of their normal ISP, and will then find that sending email fails because the configured SMTP server choice is no longer accessible.

This system has several variations. For example, an organisation's SMTP server may only provide service to users on the same network, enforcing this by firewalling to block access by users on the wider Internet. Or the server may perform range checks on the client's IP address. These methods were typically used by corporations and institutions such as universities which provided an SMTP server for outbound mail only for use internally within the organisation. However, most of these bodies now use client authentication methods, as described below.

By restricting access to certain IP addresses, server administrators can readily recognise the IP address of any abuser. As it will be a meaningful address to them, the administrators can deal with the rogue machine or user.

Where a user is mobile, and may use different ISPs to connect to the internet, this kind of usage restriction is onerous, and altering the configured outbound email SMTP server address is impractical. It is highly desirable to be able to use email client configuration information that does not need to change.

#### Client authentication

Modern SMTP servers typically require authentication of clients by credentials before allowing access, rather than restricting access by location as described earlier. This more flexible system is friendly to mobile users and allows them to have a fixed choice of configured outbound SMTP server.

#### Open relay

A server that is accessible on the wider Internet and does not enforce these kinds of access restrictions is known as an open relay. This is now generally considered a bad practice worthy of blacklisting.

#### Ports

Server administrators choose whether clients use TCP port 25 (SMTP) or port 587 (Submission), as formalized in RFC 6409 (previously RFC 2476), for relaying outbound mail to a mail server. The specifications and many servers support both. Although some servers support port 465 for legacy *secure SMTP* in violation of the specifications, it is preferable to use standard ports and standard ESMTP commands<sup>[16]</sup> according to RFC 3207 if a secure session needs to be used between the client and the server.

Some servers are set up to reject all relaying on port 25, but valid users authenticating on port 587 are allowed to relay mail to any valid address.

Some Internet service providers intercept port 25, redirecting traffic to their own SMTP server regardless of the destination address. This means that it is not possible for their users to access an SMTP server outside the ISP's network using port 25.

Some SMTP servers support authenticated access on an additional port other than 25 to allow users to connect to them even if port 25 is blocked.

## SMTP transport example

A typical example of sending a message via SMTP to two mailboxes (*alice* and *theboss*) located in the same mail domain (*example.com* or *localhost.com*) is reproduced in the following session exchange. (In this example, the conversation parts are prefixed with *S:* and *C:*, for *server* and *client*, respectively; these labels are not part of the exchange.)

After the message sender (SMTP client) establishes a reliable communications channel to the message receiver (SMTP server), the session is opened with a greeting by the server, usually containing its fully qualified domain name (FQDN), in this case *smtp.example.com*. The client initiates its dialog by responding with a `HELO` command identifying itself in the command's parameter with its FQDN (or an address literal if none is available).<sup>[2]</sup>

```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: "Alice Example" <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```

{The server closes the connection}

The client notifies the receiver of the originating email address of the message in a `MAIL FROM` command. In this example, the email message is sent to two mailboxes on the same SMTP server: one each for each recipient listed in

the `TO` and `CC` header fields. The corresponding SMTP command is `RCPT TO`. Each successful reception and execution of a command is acknowledged by the server with a result code and response message (e.g., `250 Ok`).

The transmission of the body of the mail message is initiated with a `DATA` command after which it is transmitted verbatim line by line and is terminated with an end-of-data sequence. This sequence consists of a new-line (`<CR><LF>`), a single full stop (period), followed by another new-line. Since a message body can contain a line with just a period as part of the text, the client sends *two* periods every time a line starts with a period; correspondingly, the server replaces every sequence of two periods at the beginning of a line with a single one. Such escaping method is called *dot-stuffing*.

The server's positive reply to the end-of-data, as exemplified, implies that the server has taken the responsibility of delivering the message. A message can be doubled if there is a communication failure at this time, e.g. due to a power shortage: Until the sender has received that `250` reply, it must assume the message was not delivered. On the other hand, after the receiver has decided to accept the message, it must assume the message has been delivered to it. Thus, during this time span, both agents have active copies of the message that they will try to deliver.<sup>[17]</sup> The probability that a communication failure occurs exactly at this step is directly proportional to the amount of filtering that the server performs on the message body, most often for anti-spam purposes. The limiting timeout is specified to be 10 minutes.<sup>[18]</sup>

The `QUIT` command ends the session. If the second recipient were located elsewhere, the client would `QUIT` and connect to the appropriate SMTP server after the first message had been queued. The information that the client sends in the `HELO` and `MAIL FROM` commands are added (not seen in example code) as additional header fields to the message by the receiving server. It adds a `Received` and `Return-Path` header field, respectively.

## Optional extensions

Although optional and not shown in this example, many clients ask the server for the SMTP extensions that the server supports, by using the `EHLO` greeting of the extended SMTP specification (RFC 1870). Clients fall back to `HELO` only if the server does not respond to `EHLO`.

Modern clients may use the ESMTP extension keyword `SIZE` to query the server for the maximum message size that will be accepted. Older clients and servers may try to transfer excessively sized messages that will be rejected after consuming network resources, including connect time to network links that is paid by the minute.

Users can manually determine in advance the maximum size accepted by ESMTP servers. The client replaces the `HELO` command with the `EHLO` command.

```
S: 220 smtp2.example.com ESMTP Postfix
C: EHLO bob.example.org
S: 250-smtp2.example.com Hello bob.example.org [192.0.2.201]
S: 250-SIZE 14680064
S: 250-PIPELINING
S: 250 HELP
```

Thus `smtp2.example.com` declares that it will accept a fixed maximum message size no larger than 14,680,064 octets (8-bit bytes). Depending on the server's actual resource usage, it may be currently unable to accept a message this large. In the simplest case, an ESMTP server will declare a maximum `SIZE` with only the `EHLO` user interaction.

## Security and spamming

The original SMTP specification did not include a facility for authentication of senders. Subsequently, the SMTP-AUTH extension was defined by RFC 2554.<sup>[19]</sup> The SMTP extension (ESMTP) provides a mechanism for email clients to specify a security mechanism to a mail server, authenticate the exchange, and negotiate a security profile (Simple Authentication and Security Layer, SASL) for subsequent message transfers.

Microsoft products implement the proprietary Secure Password Authentication (SPA) protocol through the use of the SMTP-AUTH extension.

However, the impracticality of widespread SMTP-AUTH implementation and management means that E-mail spamming is not and cannot be addressed by it.

Modifying SMTP extensively, or replacing it completely, is not believed to be practical, due to the network effects of the huge installed base of SMTP. Internet Mail 2000 was one such proposal for replacement.

Spam is enabled by several factors, including vendors implementing MTAs that are not standards-compliant, which make it difficult for other MTAs to enforce standards, security vulnerabilities within the operating system (often exacerbated by always-on broadband connections) that allow spammers to remotely control end-user PCs and cause them to send spam, and a lack of "intelligence" in many MTAs.

There are a number of proposals for sideband protocols that will assist SMTP operation. The Anti-Spam Research Group (ASRG) of the Internet Research Task Force (IRTF) is working on a number of E-mail authentication and other proposals for providing simple source authentication that is flexible, lightweight, and scalable. Recent Internet Engineering Task Force (IETF) activities include MARID (2004) leading to two approved IETF experiments in 2005, and DomainKeys Identified Mail in 2006.

## Related Requests For Comments

- RFC 1123 – Requirements for Internet Hosts—Application and Support (STD 3)
- RFC 1870 – SMTP Service Extension for Message Size Declaration (obsoletes: RFC 1653)
- RFC 2505 – Anti-Spam Recommendations for SMTP MTAs (BCP 30)
- RFC 2920 – SMTP Service Extension for Command Pipelining (STD 60)
- RFC 3030 – SMTP Service Extensions for Transmission of Large and Binary MIME Messages
- RFC 3207 – SMTP Service Extension for Secure SMTP over Transport Layer Security (obsoletes RFC 2487)
- RFC 3461 – SMTP Service Extension for Delivery Status Notifications (obsoletes RFC 1891)
- RFC 3463 – Enhanced Status Codes for SMTP (obsoletes RFC 1893 )
- RFC 3464 – An Extensible Message Format for Delivery Status Notifications (obsoletes RFC 1894)
- RFC 3798 - Message Disposition Notification
- RFC 3834 – Recommendations for Automatic Responses to Electronic Mail
- RFC 4952 – Overview and Framework for Internationalized E-mail
- RFC 4954 – SMTP Service Extension for Authentication (obsoletes RFC 2554)
- RFC 5068 – E-mail Submission Operations: Access and Accountability Requirements (BCP 134)
- RFC 5321 – The Simple Mail Transfer Protocol (obsoletes RFC 821 aka STD 10, RFC 974, RFC 1869, RFC 2821)
- RFC 5322 – Internet Message Format (obsoletes RFC 822 aka STD 11, and RFC 2822)
- RFC 5336 - SMTP Extension for Internationalized Email Addresses (updates RFC 2821, RFC 2822, and RFC 4952)
- RFC 5504 - Downgrading Mechanism for Email Address Internationalization
- RFC 6409 – Message Submission for Mail (obsoletes RFC 4409, RFC 2476)
- RFC 6522 – The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages (obsoletes RFC 3462, and in turn RFC 1892)

## References

- [1] RFC 821, *Simple Mail Transfer Protocol*, J.B. Postel, The Internet Society (August 1982)
- [2] RFC 5321, *Simple Mail Transfer Protocol*, J. Klensin, The Internet Society (October 2008)
- [3] The History of Electronic Mail (<http://www.multicians.org/thvv/mail-history.html>), *Tom Van Vleck*: "It is not clear this protocol was ever implemented"
- [4] *The First Network Email* (<http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html>), Ray Tomlinson, BBN
- [5] Picture of "The First Email Computer" (<http://openmap.bbn.com/~tomlinso/ray/ka10.html>) by Dan Murphy, a PDP-10
- [6] Dan Murphy's TENEX and TOPS-20 Papers (<http://www.opost.com/dlm/tenex/>)
- [7] RFC 2235
- [8] RFC 469 - Network Mail Meeting Summary
- [9] RFC 524 - A Proposed Mail Protocol
- [10] RFC 772 - Mail Transfer Protocol
- [11] Tldp.org (<http://tldp.org/HOWTO/Usenet-News-HOWTO/x64.html>)
- [12] draft-barber-uucp-project-conclusion-05 - The Conclusion of the UUCP Mapping Project (<http://tools.ietf.org/html/draft-barber-uucp-project-conclusion-05>)
- [13] Eric Allman (1983), *Sendmail - An Internetwork Mail Router* (<http://docs.freebsd.org/44doc/smm/09.sendmail/paper.pdf>), BSD UNIX documentation set, Berkeley: University of California, , retrieved 29 June 2012
- [14] Craig Partridge (2008), *The Technical Development of Internet Email* (<http://www.ir.bbn.com/~craig/email.pdf>), IEEE Annals of the History of Computing, IEEE Computer Society, doi:10.1109/MAHC.2008.32,
- [15] RFC 1985, *SMTP Service Extension for Remote Message Queue Starting*, J. De Winter, The Internet Society (August 1996)
- [16] RFC 3207 specifies only the well-known port 25 and the "Submission port," which is TCP port 587, for the STARTTLS command, the precursor for an encrypted SMTP session using TLS. It makes no mention of the unofficial port 465.
- [17] RFC 1047
- [18] rfc5321#section-4.5.3.2.6 (<http://tools.ietf.org/html/rfc5321#section-4.5.3.2.6>)
- [19] RFC 2554, *SMTP Service Extension for Authentication*, J. Myers (March 1999)

## Further reading

- Hughes, L (1998). *Internet e-mail Protocols, Standards and Implementation*. Artech House Publishers. ISBN 0-89006-939-5.
- Hunt, C (2003). *sendmail Cookbook*. O'Reilly Media. ISBN 0-596-00471-0.
- Johnson, K (2000). *Internet Email Protocols: A Developer's Guide*. Addison-Wesley Professional. ISBN 0-201-43288-9.
- Loshin, P (1999). *Essential Email Standards: RFCs and Protocols Made Practical*. John Wiley & Sons. ISBN 0-471-34597-0.
- Rhoton, J (1999). *Programmer's Guide to Internet Mail: SMTP, POP, IMAP, and LDAP*. Elsevier. ISBN 1-55558-212-5.
- Wood, D (1999). *Programming Internet Mail*. O'Reilly. ISBN 1-56592-479-7.

## External links

- Essential Internet Protocols - SMTP (<http://www.vanemery.com/Protocols/SMTP/smtp.html>)
- SMTP Sequence Diagram ([http://www.eventhelix.com/RealtimeMantra/Networking/SMTP\\_Sequence\\_Diagram.pdf](http://www.eventhelix.com/RealtimeMantra/Networking/SMTP_Sequence_Diagram.pdf)) (PDF)
- The Case For E-mail Security (<http://luxsci.com/extranet/articles/email-security.html>) - Security and Insecurity in SMTP, POP and IMAP.
- Picture of the first computers to send and receive a network email, 2 PDP-10s (<http://history-computer.com/Internet/Maturing/Tomlinson.html>)
- Email Address Internationalization IETF Working Group (<http://www.ietf.org/html.charters/eai-charter.html>)
- SMTP TLS Transport real-time test (<http://www.CheckTLS.com/TestReceiver?LEVEL=3>) - Live version of above example, mostly for TLS (i.e. secure) email but useful for non-TLS too

# Internet Message Access Protocol

---

**Internet message access protocol (IMAP)** is one of the two most prevalent Internet standard protocols for e-mail retrieval, the other being the Post Office Protocol (POP).<sup>[1]</sup> Virtually all modern e-mail clients and mail servers support both protocols as a means of transferring e-mail messages from a server.

## E-mail protocols

The Internet Message Access Protocol (commonly known as IMAP) is an Application Layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server. The current version, IMAP version 4 revision 1 (IMAP4rev1), is defined by RFC 3501<sup>[2]</sup>. An IMAP server typically listens on well-known port 143. IMAP over SSL (**IMAPS**) is assigned well-known port number 993.

IMAP supports both on-line and off-line modes of operation. E-mail clients using IMAP generally leave messages on the server until the user explicitly deletes them. This and other characteristics of IMAP operation allow multiple clients to manage the same mailbox. Most e-mail *clients* support IMAP in addition to POP to retrieve messages; however, fewer e-mail *services* support IMAP.<sup>[3]</sup> IMAP offers access to the mail storage. Clients may store local copies of the messages, but these are considered to be a temporary cache.

Incoming e-mail messages are sent to an e-mail server that stores messages in the recipient's e-mail box. The user retrieves the messages with an e-mail client that uses one of a number of e-mail retrieval protocols. Some clients and servers preferentially use vendor-specific, proprietary protocols, but most support the Internet standard protocols, SMTP for sending e-mail and POP and IMAP for retrieving e-mail, allowing interoperability with other servers and clients. For example, Microsoft's Outlook client uses a proprietary protocol to communicate with a Microsoft Exchange Server server as does IBM's Notes client when communicating with a Domino server, but all of these products also support POP, IMAP, and outgoing SMTP. Support for the Internet standard protocols allows many e-mail clients such as Pegasus Mail or Mozilla Thunderbird (see comparison of e-mail clients) to access these servers, and allows the clients to be used with other servers (see list of mail servers).

## History

IMAP was designed by Mark Crispin in 1986 as a remote mailbox protocol, in contrast to the widely used POP, a protocol for retrieving the contents of a mailbox.<sup>[4]</sup>

IMAP was previously known as **Internet Mail Access Protocol**, **Interactive Mail Access Protocol** (RFC 1064), and **Interim Mail Access Protocol**.<sup>[5]</sup>

## Original IMAP

The original *Interim Mail Access Protocol* was implemented as a Xerox Lisp machine client and a TOPS-20 server.

No copies of the original interim protocol specification or its software exist. Although some of its commands and responses were similar to IMAP2, the interim protocol lacked command/response tagging and thus its syntax was incompatible with all other versions of IMAP.

## IMAP2

The interim protocol was quickly replaced by the *Interactive Mail Access Protocol* (IMAP2), defined in RFC 1064 (in 1988) and later updated by RFC 1176 (in 1990). IMAP2 introduced command/response tagging and was the first publicly distributed version.

## IMAP3

IMAP3 is an extinct and extremely rare variant of IMAP.<sup>[6]</sup> It was published as RFC 1203 in 1991. It was written specifically as a counter proposal to RFC 1176, which itself proposed modifications to IMAP2.<sup>[7]</sup> IMAP3 was never accepted by the marketplace.<sup>[8][9]</sup> The IESG reclassified RFC1203 "Interactive Mail Access Protocol - Version 3" as a Historic protocol in 1993. The IMAP Working Group used RFC1176 (IMAP2) rather than RFC1203 (IMAP3) as its starting point.<sup>[10][11]</sup>

## IMAP2bis

With the advent of MIME, IMAP2 was extended to support MIME body structures and add mailbox management functionality (create, delete, rename, message upload) that was absent in IMAP2. This experimental revision was called IMAP2bis; its specification was never published in non-draft form. An internet draft of IMAP2bis was published by the IETF IMAP Working Group in October 1993. This draft was based upon the following earlier specifications: unpublished *IMAP2bis.TXT* document, RFC1176, and RFC1064 (IMAP2).<sup>[12]</sup> The *IMAP2bis.TXT* draft documented the state of extensions to IMAP2 as of December 1992.<sup>[13]</sup> Early versions of Pine were widely distributed with IMAP2bis support<sup>[6]</sup> (Pine 4.00 and later supports IMAP4rev1).

## IMAP4

An IMAP Working Group formed in the IETF in the early 1990s took over responsibility for the IMAP2bis design. The IMAP WG decided to rename IMAP2bis to IMAP4 to avoid confusion with a competing IMAP3 proposal from another group that never got off the ground. The expansion of the IMAP acronym also changed to the *Internet Message Access Protocol*

## Advantages over POP

### Connected and disconnected modes of operation

When using POP, clients typically connect to the e-mail server briefly, only as long as it takes to download new messages. When using IMAP4, clients often stay connected as long as the user interface is active and download message content on demand. For users with many or large messages, this IMAP4 usage pattern can result in faster response times.

## Multiple clients simultaneously connected to the same mailbox

The POP protocol requires the currently connected client to be the only client connected to the mailbox. In contrast, the IMAP protocol specifically allows simultaneous access by multiple clients and provides mechanisms for clients to detect changes made to the mailbox by other, concurrently connected, clients. See for example RFC3501 section 5.2 which specifically cites "simultaneous access to the same mailbox by multiple agents" as an example.

## Access to MIME message parts and partial fetch

Usually all Internet e-mail is transmitted in MIME format, allowing messages to have a tree structure where the leaf nodes are any of a variety of single part content types and the non-leaf nodes are any of a variety of multipart types. The IMAP4 protocol allows clients to separately retrieve any of the individual MIME parts and also to retrieve portions of either individual parts or the entire message. These mechanisms allow clients to retrieve the text portion of a message without retrieving attached files or to stream content as it is being fetched.

## Message state information

Through the use of flags defined in the IMAP4 protocol, clients can keep track of message state: for example, whether or not the message has been read, replied to, or deleted. These flags are stored on the server, so different clients accessing the same mailbox at different times can detect state changes made by other clients. POP provides no mechanism for clients to store such state information on the server so if a single user accesses a mailbox with two different POP clients (at different times), state information—such as whether a message has been accessed—cannot be synchronized between the clients. The IMAP4 protocol supports both pre-defined system flags and client-defined keywords. System flags indicate state information such as whether a message has been read. Keywords, which are not supported by all IMAP servers, allow messages to be given one or more tags whose meaning is up to the client. Adding user-created tags to messages is an operation supported by some web-based e-mail services, such as Gmail.

## Multiple mailboxes on the server

IMAP4 clients can create, rename, and/or delete mailboxes (usually presented to the user as folders) on the server, and copy messages between mailboxes. Multiple mailbox support also allows servers to provide access to shared and public folders. The *IMAP4 Access Control List (ACL) Extension* (RFC 4314) may be used to regulate access rights.

## Server-side searches

IMAP4 provides a mechanism for a client to ask the server to search for messages meeting a variety of criteria. This mechanism avoids requiring clients to download every message in the mailbox in order to perform these searches.

## Built-in extension mechanism

Reflecting the experience of earlier Internet protocols, IMAP4 defines an explicit mechanism by which it may be extended. Many extensions to the base protocol have been proposed and are in common use. IMAP2bis did not have an extension mechanism, and POP now has one defined by RFC 2449.

## Disadvantages

While IMAP remedies many of the shortcomings of POP, this inherently introduces additional complexity. Much of this complexity (e.g., multiple clients accessing the same mailbox at the same time) is compensated for by server-side workarounds such as Maildir or database backends.

The IMAP specification has been criticised for being insufficiently strict and allowing behaviours that effectively negate its usefulness. For instance, the specification states that each message stored on the server has a "unique id" to allow the clients to identify the messages they have already seen between sessions. However, the specification also

allows these UIDs to be invalidated with no restrictions, practically defeating their purpose.<sup>[14]</sup>

Unless the mail storage and searching algorithms on the server are carefully implemented, a client can potentially consume large amounts of server resources when searching massive mailboxes.

IMAP4 clients need to maintain a TCP/IP connection to the IMAP server in order to be notified of the arrival of new mail. Notification of mail arrival is done through in-band signaling, which contributes to the complexity of client-side IMAP protocol handling somewhat.<sup>[15]</sup> A private proposal, push IMAP, would extend IMAP to implement push e-mail by sending the entire message instead of just a notification. However, push IMAP has not been generally accepted and current IETF work has addressed the problem in other ways (see the Lemonade Profile for more information).

Unlike some proprietary protocols which combine sending and retrieval operations, sending a message and saving a copy in a server-side folder with a base-level IMAP client requires transmitting the message content twice, once to SMTP for delivery and a second time to IMAP to store in a sent mail folder. This is remedied by a set of extensions defined by the IETF LEMONADE Working Group for mobile devices: URLAUTH (RFC 4467) and CATENATE (RFC 4469) in IMAP and BURL (RFC 4468) in SMTP-SUBMISSION. POP servers don't support server-side folders so clients have no choice but to store sent items on the client. Many IMAP clients can be configured to store sent mail in a client-side folder, or to BCC oneself and then filter the incoming mail instead of saving a copy in a folder directly. In addition to the LEMONADE "trio", Courier Mail Server offers a non-standard method of sending using IMAP by copying an outgoing message to a dedicated outbox folder.

Like POP, IMAP is an e-mail only protocol. As a result, items such as contacts, appointments or tasks cannot be managed or accessed using IMAP.

## References

- [1] Pegoraro, Rob (2004-03-24). "Internet Providers Should Find Their Way to IMAP" (<http://www.washingtonpost.com/wp-dyn/articles/A10089-2004Mar20.html>). Washington Post. . Retrieved 2008-06-25.
- [2] <http://tools.ietf.org/html/rfc3501>
- [3] Mullet, Diana (2000). *Managing IMAP*. O'Reilly. p. 25. ISBN 0-596-00012-X.
- [4] The IMAP Connection - IMAP Status and History (<http://www.ietf.org/about/history.status.html>)
- [5] <http://www.iana.org/assignments/service-names>
- [6] "RFC 2061 - IMAP4 COMPATIBILITY WITH IMAP2BIS" (<http://tools.ietf.org/html/rfc2061>). IETF. 1996. . Retrieved 2010-08-21.
- [7] "INTERACTIVE MAIL ACCESS PROTOCOL - VERSION 3" (<http://tools.ietf.org/html/rfc1203>). IETF. 1991. . Retrieved 2010-08-21.
- [8] "IMAP2, IMAP2bis, IMAP3, IMAP4, IMAP4rev1 (LAN Mail Protocols)" (<http://stason.org/TULARC/networking/lans-mail-protocols/03-IMAP2-IMAP2bis-IMAP3-IMAP4-IMAP4rev1-LAN-Mail-Protoc.html>). . Retrieved 2010-08-21.
- [9] "IMAP Overview, History, Versions and Standards" ([http://www.tcpipguide.com/free/t\\_IMAPOverviewHistoryVersionsandStandards-3.htm](http://www.tcpipguide.com/free/t_IMAPOverviewHistoryVersionsandStandards-3.htm)). . Retrieved 2010-08-21.
- [10] "Protocol Action: Interactive Mail Access Protocol - Version 3 to Historic (IETF mail archive)" (<http://www.ietf.org/mail-archive/web/ietf/current/msg01656.html>). 1993. . Retrieved 2010-08-21.
- [11] "Innosoft and POP/IMAP protocols? (mail archive)" (<http://www.pmdf.process.com/ftp/info-pmdf/aug.1993?httpd=content&type=text/plain; charset=ISO-8859-1>). 1993. . Retrieved 2010-08-21.
- [12] "INTERACTIVE MAIL ACCESS PROTOCOL - VERSION 2bis (Internet Draft)" (<http://tools.ietf.org/html/draft-ietf-imap-imap2bis-02>). IETF. 1993. . Retrieved 2010-08-21.
- [13] "IMAP2BIS -- EXTENSIONS TO THE IMAP2 PROTOCOL (DRAFT)" (<http://ftp.zcu.cz/pub/network/imap/old/IMAP2bis.TXT>). 1992. . Retrieved 2010-08-21.
- [14] "IMAP implementation in Sup, an e-mail client written in Ruby" (<http://sup.rubyforge.org/svn/trunk/lib/sup/imap.rb>). rubyforge.com. . Retrieved 2011-02-22.
- [15] "IMAP IDLE: The best approach for 'push' e-mail" (<http://www.isode.com/whitepapers/imap-idle.html>). Isode.com. . Retrieved 2009-07-30.

## Further reading

- Heinlein, P; Hartleben, P (2008). *The Book of IMAP: Building a Mail Server with Courier and Cyrus*. No Starch Press. ISBN 1-59327-177-8.
- Hughes, L (1998). *Internet e-mail Protocols, Standards and Implementation*. Artech House Publishers. ISBN 0-89006-939-5.
- Johnson, K (2000). *Internet E-mail Protocols: A Developer's Guide*. Addison-Wesley Professional. ISBN 0-201-43288-9.
- Loshin, P (1999). *Essential E-mail Standards: RFCs and Protocols Made Practical*. John Wiley & Sons. ISBN 0-471-34597-0.
- Mullet, K (2000). *Managing IMAP*. O'Reilly Media. ISBN 0-596-00012-X.
- Rhoton, J (1999). *Programmer's Guide to Internet Mail: SMTP, POP, IMAP, and LDAP*. Elsevier. ISBN 1-55558-212-5.
- Wood, D (1999). *Programming Internet Mail*. O'Reilly. ISBN 1-56592-479-7.

## External links

- "IMAP Protocol Mailing List" (<http://www imapwiki org/ImapProtocolList>).
- RFC 3501 - specification of IMAP version 4 revision 1
- RFC 2683 - IMAP Implementation Suggestions RFC
- RFC 2177 - IMAP4 IDLE command

# Lightweight Directory Access Protocol

The **Lightweight Directory Access Protocol (LDAP)** (/'ɛldæp/) is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.<sup>[1]</sup> LDAP is defined in terms of ASN.1 and transmitted using BER.

Directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

LDAP is specified in a series of Internet Engineering Task Force (IETF) Standard Track Requests for comments (RFCs). The latest version is Version 3, published as RFC 4510.

## Origin and influences

Telecommunication companies' understanding of directory requirements was well developed after some 70 years of producing and managing telephone directories. These companies introduced the concept of directory services to information technology and computer networking, their input culminating in the comprehensive X.500 specification,<sup>[2]</sup> a suite of protocols produced by the International Telecommunication Union (ITU) in the 1980s.

X.500 directory services were traditionally accessed via the X.500 Directory Access Protocol (DAP), which required the Open Systems Interconnection (OSI) protocol stack. LDAP was originally intended to be a lightweight alternative protocol for accessing X.500 directory services through the simpler (and now widespread) TCP/IP protocol stack. This model of directory access was borrowed from the DIXIE and Directory Assistance Service protocols.

Standalone LDAP directory servers soon followed, as did directory servers supporting both DAP and LDAP. The latter has become popular in enterprises, as LDAP removed any need to deploy an OSI network. Today, X.500 directory protocols including DAP can also be used directly over TCP/IP.

The protocol was originally created by Tim Howes of the University of Michigan, Steve Kille of Isode Limited, and Wengyik Yeong of Performance Systems International, circa 1993. Mark Wahl of Critical Angle Inc., Tim Howes, and Steve Kille started work in 1996 on a new version of LDAP, LDAPv3, under the aegis of the Internet Engineering Task Force (IETF). LDAPv3, first published in 1997, superseded LDAPv2 and added support for extensibility, integrated the Simple Authentication and Security Layer, and better aligned the protocol to the 1993 edition of X.500. Further development of the LDAPv3 specifications themselves and of numerous extensions adding features to LDAPv3 has come through the IETF.

In the early engineering stages of LDAP, it was known as *Lightweight Directory Browsing Protocol*, or *LDBP*. It was renamed with the expansion of the scope of the protocol beyond directory browsing and searching, to include directory update functions. It was given its *Lightweight* name because it was not as network intensive as its DAP predecessor and thus was more easily implemented over the internet due to its relatively modest bandwidth usage.

LDAP has influenced subsequent Internet protocols, including later versions of X.500, XML Enabled Directory (XED), Directory Service Markup Language (DSML), Service Provisioning Markup Language (SPML), and the Service Location Protocol (SLP).

## Protocol overview

A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP port 389. The client then sends an operation request to the server, and the server sends responses in return. With some exceptions, the client does not need to wait for a response before sending the next request, and the server may send the responses in any order.

The client may request the following operations:

- StartTLS — use the LDAPv3 Transport Layer Security (TLS) extension for a secure connection
- Bind — authenticate and specify LDAP protocol version
- Search — search for and/or retrieve directory entries
- Compare — test if a named entry contains a given attribute value
- Add a new entry
- Delete an entry
- Modify an entry
- Modify Distinguished Name (DN) — move or rename an entry
- Abandon — abort a previous request
- Extended Operation — generic operation used to define other operations
- Unbind — close the connection (not the inverse of Bind)

In addition the server may send "Unsolicited Notifications" that are not responses to any request, e.g. before it times out a connection.

A common alternative method of securing LDAP communication is using an SSL tunnel. This is denoted in LDAP URLs by using the URL scheme "ldaps". The default port for LDAP over SSL is 636. The use of LDAP over SSL was common in LDAP Version 2 (LDAPv2) but it was never standardized in any formal specification. This usage has been deprecated along with LDAPv2, which was officially retired in 2003.<sup>[3]</sup>

## Directory structure

The protocol accesses LDAP directories, which follow the 1993 edition of the X.500 model:

- An entry consists of a set of attributes.
- An attribute has a name (an *attribute type* or *attribute description*) and one or more values. The attributes are defined in a *schema* (see below).
- Each entry has a unique identifier: its *Distinguished Name* (DN). This consists of its *Relative Distinguished Name* (RDN), constructed from some attribute(s) in the entry, followed by the parent entry's DN. Think of the DN as the full file path and the RDN as its relative filename in its parent folder (e.g. if `/foo/bar/myfile.txt` were the DN, then `myfile.txt` would be the RDN).

Be aware that a DN may change over the lifetime of the entry, for instance, when entries are moved within a tree. To reliably and unambiguously identify entries, a UUID might be provided in the set of the entry's *operational attributes*.

An entry can look like this when represented in LDAP Data Interchange Format (LDIF) (LDAP itself is a binary protocol):

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

"dn" is the distinguished name of the entry; it's neither an attribute nor a part of the entry. "cn=John Doe" is the entry's RDN (Relative Distinguished Name), and "dc=example,dc=com" is the DN of the parent entry, where "dc" denotes 'Domain Component'. The other lines show the attributes in the entry. Attribute names are typically mnemonic strings, like "cn" for common name, "dc" for domain component, "mail" for e-mail address and "sn" for surname.

A server holds a subtree starting from a specific entry, e.g. "dc=example,dc=com" and its children. Servers may also hold references to other servers, so an attempt to access "ou=department,dc=example,dc=com" could return a *referral* or *continuation reference* to a server that holds that part of the directory tree. The client can then contact the other server. Some servers also support *chaining*, which means the server contacts the other server and returns the results to the client.

LDAP rarely defines any ordering: The server may return the values of an attribute, the attributes in an entry, and the entries found by a search operation in any order. This follows from the formal definitions - an entry is defined as a set of attributes, and an attribute is a set of values, and sets need not be ordered.

## Operations

*Expand discussion of referral responses to various operations, especially modify, for example where all modifications must be directed from replicas to a master directory.*

### Add

The ADD operation inserts a new entry into the directory-server database.<sup>[4]</sup> If the distinguished name in the add request already exists in the directory, then the server will not add a duplicate entry but will set the result code in the add result to decimal 68, "entryAlreadyExists".<sup>[5]</sup>

- LDAP-compliant servers will never dereference the distinguished name transmitted in the add request when attempting to locate the entry, that is, distinguished names are never de-aliased.
- LDAP-compliant servers will ensure that the distinguished name and all attributes conform to naming standards
- The entry to be added must not exist, and the immediate superior must exist.

```
dn: uid=user,ou=people,dc=example,dc=com
changetype: add
objectClass: top
objectClass: person
uid: user
sn: last-name
cn: common-name
userPassword: password
```

In the above example, `uid=user,ou=people,dc=example,dc=com` must not exist, and `ou=people,dc=example,dc=com` must exist.

### Bind (authenticate)

When an LDAP session is created, that is, when an LDAP client connects to the server, the **authentication state** of the session is set to anonymous. The BIND operation establishes the authentication state for a session.

Simple BIND and SASL PLAIN can send the user's DN and password in plaintext, so the connections utilizing either Simple or SASL PLAIN should be encrypted using Transport Layer Security (TLS). The server typically checks the password against the `userPassword` attribute in the named entry. Anonymous BIND (with empty DN and password) resets the connection to anonymous state.

SASL (Simple Authentication and Security Layer) BIND provides authentication services through a wide range of mechanisms, e.g. Kerberos or the client certificate sent with TLS.<sup>[6]</sup>

BIND also sets the LDAP protocol version. The version is an integer and at present must be either 2 (two) or 3 (three), although the standard supports integers between 1 and 127 (inclusive) in the protocol. If the client requests a version that the server does not support, the server must set the result code in the BIND response to the code for a protocol error. Normally clients should use LDAPv3, which is the default in the protocol but not always in LDAP libraries.

BIND had to be the first operation in a session in LDAPv2, but is not required in LDAPv3 (the current LDAP version). In LDAPv3, each successful BIND request changes the authentication state of the session and each unsuccessful BIND request resets the authentication state of the session.

## Delete

To delete an entry, an LDAP client transmits a properly formed delete request to the server.<sup>[7]</sup>

- A delete request must contain the distinguished name of the entry to be deleted
- Request controls may also be attached to the delete request
- Servers do not dereference aliases when processing a delete request
- Only leaf nodes (entries with no subordinates) may be deleted by a delete request. Some servers support an operational attribute `hasSubordinates` whose value indicates whether an entry has any subordinate entries, and some servers support an operational attribute `numSubordinates`<sup>[8]</sup> indicating the number of entries subordinate to the entry containing the `numSubordinates` attribute.

Delete requests are subject to access controls, that is, whether a connection with a given authentication state will be permitted to delete a given entry is governed by server-specific access control mechanisms.

## Search and Compare

The Search operation is used to both search for and read entries. Its parameters are:

`baseObject`

The name of the base object entry (or possibly the root) relative to which the search is to be performed.

`scope`

What elements below the `baseObject` to search. This can be `BaseObject` (search just the named entry, typically used to read one entry), `singleLevel` (entries immediately below the base DN), or `wholeSubtree` (the entire subtree starting at the base DN).

`filter`

Criteria to use in selecting elements within scope. For example, the filter  
`(& (objectClass=person) (| (givenName=John) (mail=john*)) )` will select "persons" (elements of `objectClass person`) where the matching rules for `givenName` and `mail` determine whether the values for those attributes match the filter assertion. Note that a common misconception is that LDAP data is case-insensitive, whereas in fact matching rules and ordering rules determine matching, comparisons, and relative value relationships. If the example filters were required to match the case of the attribute value, an *extensible match filter* must be used, for example,  
`(& (objectClass=person) (| (givenName:caseExactMatch:=John) (mail:caseExactSubstringsMatch:=John*) )`

`derefAliases`

Whether and how to follow alias entries (entries that refer to other entries),

`attributes`

Which attributes to return in result entries.

`sizeLimit, timeLimit`

Maximum number of entries to return, and maximum time to allow search to run. These values, however, cannot override any restrictions the server places on size limit and time limit.

`typesOnly`

Return attribute types only, not attribute values.

The server returns the matching entries and potentially continuation references. These may be returned in any order. The final result will include the result code.

The Compare operation takes a DN, an attribute name and an attribute value, and checks if the named entry contains that attribute with that value.

## Modify

The MODIFY operation is used by LDAP clients to request that the LDAP make changes to existing entries.<sup>[9]</sup> Attempts to modify entries that do not exist will fail. MODIFY requests are subject to access controls as implemented by the server.

The MODIFY operation requires that the distinguished name (DN) of the entry be specified, and a sequence of changes. Each change in the sequence must be one of:

- add (add a new value, which must not already exist in the entry)
- delete (delete an existing value)
- replace (replace an existing value with a new value)

LDIF example of adding a value to an attribute:

```
dn: dc=example,dc=com
changetype: modify
add: cn
cn: the-new-cn-value-to-be-added
```

To replace the value of an existing attribute, Use the `replace` keyword. If the attribute is multi-valued, the client must specify the value of the attribute to delete.

To delete an attribute from an entry, use the keyword `delete` and the changetype designator `modify`. If the attribute is multi-valued, the client must specify the value of the attribute to delete.

There is also a modify-increment extension which allows an incrementable attribute value to be incremented by a specified amount. The modify-increment extension uses object identifier 1.3.6.1.1.14. The following example using LDIF increments `employeeNumber` by 5:

```
dn: uid=user.0,ou=people,dc=example,dc=com
changetype: modify
increment: employeeNumber
employeeNumber: 5
```

When LDAP servers are in a replicated topology, LDAP clients should consider using the post-read control to verify updates instead of a search after an update.<sup>[10]</sup> The post-read control is designed so that applications need not issue a search request after an update – it is bad form to retrieve an entry for the sole purpose of checking that an update worked because of the replication eventual consistency model. An LDAP client should not assume that it connects to the same directory server for each request because architects may have placed load-balancers or LDAP proxies or both between LDAP clients and servers.

## Modify DN

Modify DN (move/rename entry) takes the new RDN (Relative Distinguished Name), optionally the new parent's DN, and a flag that says whether to delete the value(s) in the entry that match the old RDN. The server may support renaming of entire directory subtrees.

An update operation is atomic: Other operations will see either the new entry or the old one. On the other hand, LDAP does not define transactions of multiple operations: If you read an entry and then modify it, another client may have updated the entry in the meantime. Servers may implement extensions<sup>[11]</sup> that support this, though.

## Extended operations

The Extended Operation is a generic LDAP operation that can define new operations that were not part of the original protocol specification. StartTLS is one of the most significant extensions. Other examples include the Cancel and Password Modify.

### StartTLS

The StartTLS operation establishes Transport Layer Security (the descendant of SSL) on the connection. It can provide data confidentiality (to protect data from being observed by third parties) and/or data integrity protection (which protects the data from tampering). During TLS negotiation the server sends its X.509 certificate to prove its identity. The client may also send a certificate to prove its identity. After doing so, the client may then use SASL/EXTERNAL. By using the SASL/EXTERNAL, the client requests the server derive its identity from credentials provided at a lower level (such as TLS). Though technically the server may use any identity information established at any lower level, typically the server will use the identity information established by TLS.

Servers also often support the non-standard "LDAPS" ("Secure LDAP", commonly known as "LDAP over SSL") protocol on a separate port, by default 636. LDAPS differs from LDAP in two ways: 1) upon connect, the client and server establish TLS before any LDAP messages are transferred (without a StartTLS operation) and 2) the LDAPS connection must be closed upon TLS closure.

It should be noted that some "LDAPS" client libraries only encrypt communication, they do not check the host name against the name in the supplied certificate<sup>[12]</sup>

LDAPS was used with LDAPv2, because the StartTLS operation had not yet been defined. The use of LDAPS is deprecated, and modern software should only use StartTLS.

### Abandon

The Abandon operation requests that the server abort an operation named by a message ID. The server need not honor the request. Unfortunately, neither Abandon nor a successfully abandoned operation send a response. A similar Cancel extended operation does send responses, but not all implementations support this.

### Unbind

The Unbind operation abandons any outstanding operations and closes the connection. It has no response. The name is of historical origin, and is *not* the opposite of the Bind operation.<sup>[13]</sup>

Clients can abort a session by simply closing the connection, but they should use Unbind.<sup>[14]</sup> Unbind allows the server to gracefully close the connection and free resources that it would otherwise keep for some time until discovering the client had abandoned the connection. It also instructs the server to cancel operations that can be canceled, and to not send responses for operations that cannot be canceled.<sup>[15]</sup>

## LDAP URLs

An LDAP URL format exists, which clients support in varying degrees, and servers return in referrals and continuation references (see RFC 4516):

```
ldap://host:port/DN?attributes?scope?filter?extensions
```

Most of the components described below are optional.

- *host* is the FQDN or IP address of the LDAP server to search.
- *port* is the network port (default port 389) of the LDAP server.
- *DN* is the distinguished name to use as the search base.
- *attributes* is a comma-separated list of attributes to retrieve.

- *scope* specifies the search scope and can be "base" (the default), "one" or "sub".
- *filter* is a search filter. For example (`objectClass=*`) as defined in RFC 4515.
- *extensions* are extensions to the LDAP URL format.

For example, "`ldap://ldap.example.com/cn=John%20Doe,dc=example,dc=com`" refers to all user attributes in John Doe's entry in `ldap.example.com`, while "`ldap:///dc=example,dc=com??sub?(givenName=John)`" searches for the entry in the default server (note the triple slash, omitting the host, and the double question mark, omitting the attributes). As in other URLs, special characters must be percent-encoded.

There is a similar non-standard `ldaps:` URL scheme for LDAP over SSL. This should not be confused with LDAP with TLS, which is achieved using the StartTLS operation using the standard `ldap:` scheme.

## Schema

The contents of the entries in a subtree are governed by a schema known as a directory information tree (DIT).

The schema of a Directory Server defines a set of rules that govern the kinds of information that the server can hold. It has a number of elements, including:

- Attribute Syntaxes—Provide information about the kind of information that can be stored in an attribute.
- Matching Rules—Provide information about how to make comparisons against attribute values.
- Matching Rule Uses—Indicate which attribute types may be used in conjunction with a particular matching rule.
- Attribute Types—Define an object identifier (OID) and a set of names that may be used to refer to a given attribute, and associates that attribute with a syntax and set of matching rules.
- Object Classes—Define named collections of attributes and classify them into sets of required and optional attributes.
- Name Forms—Define rules for the set of attributes that should be included in the RDN for an entry.
- Content Rules—Define additional constraints about the object classes and attributes that may be used in conjunction with an entry.
- Structure Rule—Define rules that govern the kinds of subordinate entries that a given entry may have.

Attributes are the elements responsible for storing information in a directory, and the schema defines the rules for which attributes may be used in an entry, the kinds of values that those attributes may have, and how clients may interact with those values.

Clients may learn about the schema elements that the server supports by retrieving an appropriate subschema subentry.

The schema defines *object classes*. Each entry must have an `objectClass` attribute, containing named classes defined in the schema. The schema definition of the classes of an entry defines what kind of object the entry may represent - e.g. a person, organization or domain. The object class definitions also define the list of attributes that must contain values and the list of attributes which may contain values.

For example, an entry representing a person might belong to the classes "top" and "person". Membership in the "person" class would require the entry to contain the "sn" and "cn" attributes, and allow the entry also to contain "userPassword", "telephoneNumber", and other attributes. Since entries may have multiple `ObjectClasses` values, each entry has a complex of optional and mandatory attribute sets formed from the union of the object classes it represents. `ObjectClasses` can be inherited, and a single entry can have multiple `ObjectClasses` values that define the available and required attributes of the entry itself. A parallel to the schema of an `objectClass` is a class definition and an instance in Object-oriented programming, representing LDAP `objectClass` and LDAP entry, respectively.

Directory servers may publish the directory schema controlling an entry at a base DN given by the entry's `subschemaSubentry` operational attribute. (An *operational attribute* describes operation of the directory rather than user information and is only returned from a search when it is explicitly requested.)

Server administrators can add additional schema entries in addition to the provided schema elements. A schema for representing individual people within organizations is termed a white pages schema.

## Variations

A lot of the server operation is left to the implementor or administrator to decide. Accordingly, servers may be set up to support a wide variety of scenarios.

For example, data storage in the server is not specified - the server may use flat files, databases, or just be a gateway to some other server. Access control is not standardized, though there has been work on it and there are commonly used models. Users' passwords may be stored in their entries or elsewhere. The server may refuse to perform operations when it wishes, and impose various limits.

Most parts of LDAP are extensible. Examples: One can define new operations. *Controls* may modify requests and responses, e.g. to request sorted search results. New search scopes and Bind methods can be defined. Attributes can have *options* that may modify their semantics.

## Other data models

As LDAP has gained momentum, vendors have provided it as an access protocol to other services. The implementation then recasts the data to mimic the LDAP/X.500 model, but how closely this model is followed varies. For example, there is software to access SQL databases through LDAP, even though LDAP does not readily lend itself to this.<sup>[16]</sup> X.500 servers may support LDAP as well.

Similarly, data previously held in other types of data stores are sometimes moved to LDAP directories. For example, Unix user and group information can be stored in LDAP and accessed via PAM and NSS modules. LDAP is often used by other services for authentication.

An example of such data model is the GLUE Schema,<sup>[17]</sup> which is used in a distributed information system based on LDAP that enable users, applications and services to discover which services exist in a Grid infrastructure and further information about their structure and state.

## Usage

An LDAP server may return referrals to other servers for requests that it cannot fulfill itself. This requires a naming structure for LDAP entries so one can find a server holding a given DN or distinguished name, a concept defined in the X.500 Directory and also used in LDAP. Another way of locating LDAP servers for an organization is a DNS server resource record (SRV).

An organization with the domain example.org may use the top level LDAP DN dc=example,dc=org (where *dc* means domain component). If the LDAP server is also named ldap.example.org, the organization's top level LDAP URL becomes ldap://ldap.example.org/dc=example,dc=org.

Primarily two common styles of naming are used in both X.500 [2008] and LDAPv3. These are documented in the ITU specifications and IETF RFCs. The original form takes the top level object as the country object, such as c=US, c=FR. The domain component model uses the model described above. An example of country based naming could be c=FR, o=Some Organization, ou=Some Organizational Unit L=Locality, or in the US: c=US, st=CA, o=Some Organization ou=Organizational Unit, L=Locality, and CN=Common Name.

## References

- [1] LDAP: Framework, Practices, and Trends (<http://www2.computer.org/portal/web/csdl/doi/10.1109/MIC.2004.44>)
- [2] The X.500 series - ITU-T Rec. X.500 to X.521
- [3] RFC3494 (<http://tools.ietf.org/html/rfc3494>)
- [4] Add section of RFC4511 (<http://tools.ietf.org/html/rfc4511#section-4.7>)
- [5] LDAP result codes (<http://tools.ietf.org/html/rfc4511#appendix-A>)
- [6] SASL Mechanisms at IANA (<http://www.iana.org/assignments/sasl-mechanisms/sasl-mechanisms.xml>)
- [7] RFC4511: delete request (<http://tools.ietf.org/html/rfc4511#section-4.8>)
- [8] Boreham Draft (numSubordinates) (<http://tools.ietf.org/html/draft-boreham-numsubordinates-01>)
- [9] Modify Section of RFC4511 (<http://tools.ietf.org/html/rfc4511#section-4.6>)
- [10] read-entry controls (<http://tools.ietf.org/html/rfc4527>)
- [11] INTERNET-DRAFT LDAP Transactions draft-zeilenga-ldap-txn-15.txt (<http://www.rfc-editor.org/internet-drafts/draft-zeilenga-ldap-txn-15.txt>)
- [12] Shibboleth Security alert 20120227 ([http://shibboleth.internet2.edu/secadv/secadv\\_20120227.txt](http://shibboleth.internet2.edu/secadv/secadv_20120227.txt))
- [13] Tools.ietf.org (<http://tools.ietf.org/html/rfc4511#section-4.3>)
- [14] Tools.ietf.org (<http://tools.ietf.org/html/rfc4511#section-5.3>)
- [15] Tools.ietf.org (<http://tools.ietf.org/html/rfc4511#section-3.1>)
- [16] Openldap.org (<http://www.openldap.org/doc/admin24/backends.html#SQL>)
- [17] SourceForge : Project Home (<http://forge.gridforum.org/sf/projects/glue-wg>)
- ITU-T Rec. X.680, "Abstract Syntax Notation One (ASN.1) - Specification of Basic Notation", 1994
- Basic encoding rules (BER) - ITU-T Rec. X.690, "Specification of ASN.1 encoding rules: Basic, Canonical, and Distinguished Encoding Rules", 1994
- RFC 3641 - Generic String Encoding Rules (GSER) for ASN.1 Types
- RFC 4346 - The TLS Protocol Version 1.1
- RFC 4422 - Simple Authentication and Security Layer (SASL)
- SASL mechanisms (<http://www.iana.org/assignments/sasl-mechanisms>) registered at IANA
- This article is based on material taken from the Free On-line Dictionary of Computing prior to 1 November 2008 and incorporated under the "relicensing" terms of the GFDL, version 1.3 or later.

## Further reading

- Arkills, B (2003). *LDAP Directories Explained: An Introduction and Analysis* (<http://www.informit.com/store/product.aspx?isbn=0-201-78792-X>). Addison-Wesley Professional. ISBN 0-201-78792-X.
- Carter, G (2003). *LDAP System Administration* (<http://oreilly.com/catalog/9781565924918>). O'Reilly Media. ISBN 1-56592-491-6.
- Donley, C (2002). *LDAP Programming, Management, and Integration*. Manning Publications. ISBN 1-930110-40-5.
- Howes, T; Smith, M; Good, G (2003). *Understanding and Deploying LDAP Directory Services* (<http://www.informit.com/store/product.aspx?isbn=0-672-32316-8>). Addison-Wesley Professional. ISBN 0-672-32316-8.
- Rhoton, J (1999). *Programmer's Guide to Internet Mail: SMTP, POP, IMAP, and LDAP*. Elsevier. ISBN 1-55558-212-5.
- Voglmaier, R (2003). *The ABCs of LDAP: How to Install, Run, and Administer LDAP Services*. Auerbach Publications. ISBN 0-8493-1346-5.

## External links

- Devshed.com (<http://www.devshed.com/c/a/Administration/Understanding-LDAP-part-1/>), Understanding LDAP, A simple, light introductory tutorial for LDAP.
- Skills-1st.co.uk (<http://www.skills-1st.co.uk/papers/ldap-schema-design-feb-2005/index.html>), LDAP schema design
- Capitalhead.com (<http://capitalhead.com/articles/troubleshooting-ldap-ssl-connection-issues-between-microsoft-ilmmiis--novell-edirectory-873.aspx>), Troubleshooting LDAP SSL connection issues between Microsoft ILM/MIIS & Novell eDirectory 8.7.3
- Prasannatech.com (<http://web.archive.org/web/20080713040421/http://www.prasannatech.com/ldapdesign.html>), LDAP schema design - A Case Study

## RFCs

LDAP is specified in a series of Request for Comments documents:

- RFC 4510 - LDAP: Technical Specification Road Map (Obsoletes: RFC 2251, RFC 2252, RFC 2253, RFC 2254, RFC 2255, RFC 2256, RFC 2829, RFC 2830, RFC 3377, RFC 3771)
- RFC 4511 - LDAP: The Protocol (Obsoletes RFC 2251, RFC 2830 & RFC 3771)
- RFC 4512 - LDAP: Directory Information Models (Obsoletes RFC 2251, RFC 2252, RFC 2256 & RFC 3674)
- RFC 4513 - LDAP: Authentication Methods and Security Mechanisms (Obsoletes RFC 2251, RFC 2829 & RFC 2830)
- RFC 4514 - LDAP: String Representation of Distinguished Names (Obsoletes RFC 2253)
- RFC 4515 - LDAP: String Representation of Search Filters (Obsoletes RFC 2254)
- RFC 4516 - LDAP: Uniform Resource Locator (Obsoletes RFC 2255)
- RFC 4517 - LDAP: Syntaxes and Matching Rules (Obsoletes RFC 2252 & RFC 2256, Updates RFC 3698)
- RFC 4518 - LDAP: Internationalized String Preparation
- RFC 4519 - LDAP: Schema for User Applications (Obsoletes RFC 2256, Updates RFC 2247, RFC 2798 & RFC 2377)

The following RFCs detail LDAP-specific Best Current Practices:

- RFC 4520 (also BCP 64) - Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP) (replaced RFC 3383)
- RFC 4521 (also BCP 118) - Considerations for Lightweight Directory Access Protocol (LDAP) Extensions

The following is a partial list of RFCs specifying LDAPv3 extensions:

- RFC 2247 - Use of DNS domains in distinguished names (Updated by RFC 4519 & RFC 4524)
- RFC 2307 - Using LDAP as a Network Information Service
- RFC 2589 - LDAPv3: Dynamic Directory Services Extensions
- RFC 2649 - LDAPv3 Operational Signatures
- RFC 2696 - LDAP Simple Paged Result Control
- RFC 2798 - inetOrgPerson LDAP Object Class (Updated by RFC 3698, RFC 4519 & RFC 4524)
- RFC 2830 - LDAPv3: Extension for Transport Layer Security
- RFC 2849 - The LDAP Data Interchange Format (LDIF)
- RFC 2891 - Server Side Sorting of Search Results
- RFC 3045 - Storing Vendor Information in the LDAP root DSE
- RFC 3062 - LDAP Password Modify Extended Operation
- RFC 3296 - Named Subordinate References in LDAP Directories
- RFC 3671 - Collective Attributes in LDAP
- RFC 3672 - Subentries in LDAP
- RFC 3673 - LDAPv3: All Operational Attributes

- RFC 3687 - LDAP Component Matching Rules
- RFC 3698 - LDAP: Additional Matching Rules
- RFC 3829 - LDAP Authorization Identity Controls
- RFC 3866 - Language Tags and Ranges in LDAP
- RFC 3909 - LDAP Cancel Operation
- RFC 3928 - LDAP Client Update Protocol
- RFC 4370 - LDAP Proxied Authorization Control
- RFC 4373 - LBURP
- RFC 4403 - LDAP Schema for UDDI
- RFC 4522 - LDAP: Binary Encoding Option
- RFC 4523 - LDAP: X.509 Certificate Schema
- RFC 4524 - LDAP: COSINE Schema (replaces RFC 1274)
- RFC 4525 - LDAP: Modify-Increment Extension
- RFC 4526 - LDAP: Absolute True and False Filters
- RFC 4527 - LDAP: Read Entry Controls
- RFC 4528 - LDAP: Assertion Control
- RFC 4529 - LDAP: Requesting Attributes by Object Class
- RFC 4530 - LDAP: entryUUID
- RFC 4531 - LDAP Turn Operation
- RFC 4532 - LDAP Who am I? Operation
- RFC 4533 - LDAP Content Sync Operation
- RFC 4876 - Configuration Profile Schema for LDAP-Based Agents
- RFC 5020 - LDAP entryDN Operational Attribute

LDAPv2 was specified in the following RFCs:

- RFC 1777 - Lightweight Directory Access Protocol (replaced RFC 1487)
- RFC 1778 - The String Representation of Standard Attribute Syntaxes (replaced RFC 1488)
- RFC 1779 - A String Representation of Distinguished Names (replaced RFC 1485)

LDAPv2 was moved to historic status by the following RFC:

- RFC 3494 - Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status
-

# Routing

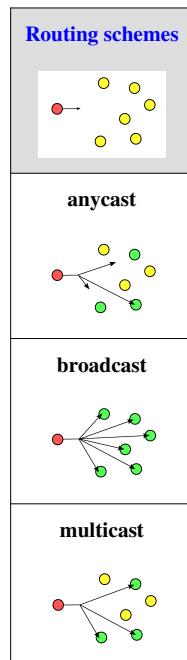
## Routing

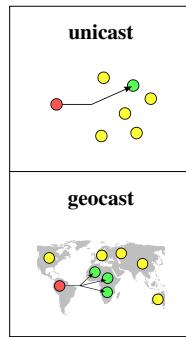
**Routing** is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network (Circuit switching), electronic data networks (such as the Internet), and transportation networks. This article is concerned primarily with routing in electronic data networks using packet switching technology.

In packet switching networks, routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes, typically hardware devices called routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time, but multipath routing techniques enable the use of multiple alternative paths.

Routing, in a more narrow sense of the term, is often contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Because structured addresses allow a single routing table entry to represent the route to a group of devices, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging) in large networks, and has become the dominant form of addressing on the Internet, though bridging is still widely used within localized environments.

### Delivery semantics





Routing schemes differ in their delivery semantics:

- unicast delivers a message to a single specific node;
- broadcast delivers a message to all nodes in the network;
- multicast delivers a message to a group of nodes that have expressed interest in receiving the message;
- anycast delivers a message to any one out of a group of nodes, typically the one nearest to the source.
- geocast delivers a message to a geographic area

Unicast is the dominant form of message delivery on the Internet, and this article focuses on unicast routing algorithms.

## Topology distribution

In a practice known as static routing (or non-adaptive routing), small networks may use manually configured routing tables. Larger networks have complex topologies that can change rapidly, making the manual construction of routing tables unfeasible. Nevertheless, most of the public switched telephone network (PSTN) uses pre-computed routing tables, with fallback routes if the most direct route becomes blocked (see routing in the PSTN). Adaptive routing, or dynamic routing, attempts to solve this problem by constructing routing tables automatically, based on information carried by routing protocols, and allowing the network to act nearly autonomously in avoiding network failures and blockages.

Examples of adaptive-routing algorithms are the Routing Information Protocol (RIP) and the Open-Shortest-Path-First protocol (OSPF). Adaptive routing dominates the Internet. However, the configuration of the routing protocols often requires a skilled touch; networking technology has not developed to the point of the complete automation of routing.

## Distance vector algorithms

Distance vector algorithms use the Bellman-Ford algorithm. This approach assigns a number, the *cost*, to each of the links between each node in the network. Nodes will send information from point A to point B via the path that results in the lowest *total cost* (i.e. the sum of the costs of the links between the nodes used).

The algorithm operates in a very simple manner. When a node first starts, it only knows of its immediate neighbours, and the direct cost involved in reaching them. (This information, the list of destinations, the total cost to each, and the *next hop* to send data to get there, makes up the routing table, or *distance table*.) Each node, on a regular basis, sends to each neighbour its own current idea of the total cost to get to all the destinations it knows of. The neighbouring node(s) examine this information, and compare it to what they already 'know'; anything which represents an improvement on what they already have, they insert in their own routing table(s). Over time, all the nodes in the network will discover the best next hop for all destinations, and the best total cost.

When one of the nodes involved goes down, those nodes which used it as their next hop for certain destinations discard those entries, and create new routing-table information. They then pass this information to all adjacent nodes, which then repeat the process. Eventually all the nodes in the network receive the updated information, and will then discover new paths to all the destinations which they can still "reach".

## Link-state algorithms

When applying link-state algorithms, each node uses as its fundamental data a map of the network in the form of a graph. To produce this, each node floods the entire network with information about what other nodes it can connect to, and each node then independently assembles this information into a map. Using this map, each router then independently determines the least-cost path from itself to every other node using a standard shortest paths algorithm such as Dijkstra's algorithm. The result is a tree rooted at the current node such that the path through the tree from the root to any other node is the least-cost path to that node. This tree then serves to construct the routing table, which specifies the best next hop to get from the current node to any other node.

## Optimised Link State Routing algorithm

A link-state routing algorithm optimised for mobile ad-hoc networks is the *Optimised Link State Routing Protocol (OLSR)*.<sup>[1]</sup> OLSR is proactive; it uses Hello and Topology Control (TC) messages to discover and disseminate link state information through the mobile ad-hoc network. Using Hello messages, each node discovers 2-hop neighbor information and elects a set of *multipoint relays* (MPRs). MPRs distinguish OLSR from other link state routing protocols.

## Path vector protocol

Distance vector and link state routing are both intra-domain routing protocols. They are used inside an autonomous system, but not between autonomous systems. Both of these routing protocols become intractable in large networks and cannot be used in Inter-domain routing. Distance vector routing is subject to instability if there are more than a few hops in the domain. Link state routing needs huge amount of resources to calculate routing tables. It also creates heavy traffic due to flooding.

Path vector routing is used for inter-domain routing. It is similar to distance vector routing. In path vector routing we assume there is one node (there can be many) in each autonomous system which acts on behalf of the entire autonomous system. This node is called the speaker node. The speaker node creates a routing table and advertises it to neighboring speaker nodes in neighboring autonomous systems. The idea is the same as distance vector routing except that only speaker nodes in each autonomous system can communicate with each other. The speaker node advertises the path, not the metric of the nodes, in its autonomous system or other autonomous systems. Path vector routing is discussed in RFC 1322; the path vector routing algorithm is somewhat similar to the distance vector algorithm in the sense that each border router advertises the destinations it can reach to its neighboring router. However, instead of advertising networks in terms of a destination and the distance to that destination, networks are advertised as destination addresses and path descriptions to reach those destinations. A route is defined as a pairing between a destination and the attributes of the path to that destination, thus the name, path vector routing, where the routers receive a vector that contains paths to a set of destinations. The path, expressed in terms of the domains (or confederations) traversed so far, is carried in a special path attribute that records the sequence of routing domains through which the reachability information has passed.

## Comparison of routing algorithms

Distance-vector routing protocols are simple and efficient in small networks and require little, if any, management. However, traditional distance-vector algorithms have poor convergence properties due to the count-to-infinity problem.

This has led to the development of more complex but more scalable algorithms for use in large networks. Interior routing mostly uses link-state routing protocols such as OSPF and IS-IS.

A more recent development is that of loop-free distance-vector protocols (e.g., EIGRP). Loop-free distance-vector protocols are as robust and manageable as naive distance-vector protocols, but avoid counting to infinity, and have good worst-case convergence times.

## Path selection

Path selection involves applying a routing metric to multiple routes, in order to select (or predict) the best route.

In the case of computer networking, the metric is computed by a routing algorithm, and can cover such information as bandwidth, network delay, hop count, path cost, load, MTU, reliability, and communication cost (see e.g. this survey<sup>[2]</sup> for a list of proposed routing metrics). The routing table stores only the best possible routes, while link-state or topological databases may store all other information as well.

Because a routing metric is specific to a given routing protocol, multi-protocol routers must use some external heuristic in order to select between routes learned from different routing protocols. Cisco's routers, for example, attribute a value known as the administrative distance to each route, where smaller administrative distances indicate routes learned from a supposedly more reliable protocol.

A local network administrator, in special cases, can set up host-specific routes to a particular machine which provides more control over network usage, permits testing and better overall security. This can come in handy when required to debug network connections or routing tables.

## Multiple agents

In some networks, routing is complicated by the fact that no single entity is responsible for selecting paths: instead, multiple entities are involved in selecting paths or even parts of a single path. Complications or inefficiency can result if these entities choose paths to optimize their own objectives, which may conflict with the objectives of other participants.

A classic example involves traffic in a road system, in which each driver picks a path which minimizes their own travel time. With such routing, the equilibrium routes can be longer than optimal for all drivers. In particular, Braess paradox shows that adding a new road can *lengthen* travel times for all drivers.

In another model, for example used for routing automated guided vehicles (AGVs) on a terminal, reservations are made for each vehicle to prevent simultaneous use of the same part of an infrastructure. This approach is also referred to as context-aware routing.<sup>[3]</sup>

The Internet is partitioned into autonomous systems (ASs) such as internet service providers (ISPs), each of which has control over routes involving its network, at multiple levels. First, AS-level paths are selected via the BGP protocol, which produces a sequence of ASs through which packets will flow. Each AS may have multiple paths, offered by neighboring ASs, from which to choose. Its decision often involves business relationships with these neighboring ASs,<sup>[4]</sup> which may be unrelated to path quality or latency. Second, once an AS-level path has been selected, there are often multiple corresponding router-level paths, in part because two ISPs may be connected in multiple locations. In choosing the single router-level path, it is common practice for each ISP to employ hot-potato routing: sending traffic along the path that minimizes the distance through the ISP's own network—even if that path lengthens the total distance to the destination.

Consider two ISPs, *A* and *B*, which each have a presence in New York, connected by a fast link with latency 5 ms; and which each have a presence in London connected by a 5 ms link. Suppose both ISPs have trans-Atlantic links connecting their two networks, but *A*'s link has latency 100 ms and *B*'s has latency 120 ms. When routing a message from a source in *A*'s London network to a destination in *B*'s New York network, *A* may choose to immediately send the message to *B* in London. This saves *A* the work of sending it along an expensive trans-Atlantic link, but causes the message to experience latency 125 ms when the other route would have been 20 ms faster.

A 2003 measurement study of Internet routes found that, between pairs of neighboring ISPs, more than 30% of paths have inflated latency due to hot-potato routing, with 5% of paths being delayed by at least 12 ms. Inflation due to AS-level path selection, while substantial, was attributed primarily to BGP's lack of a mechanism to directly optimize for latency, rather than to selfish routing policies. It was also suggested that, were an appropriate mechanism in place, ISPs would be willing to cooperate to reduce latency rather than use hot-potato routing.<sup>[5]</sup>

Such a mechanism was later published by the same authors, first for the case of two ISPs<sup>[6]</sup> and then for the global case.<sup>[7]</sup>

## Route analytics

As the Internet and IP networks become mission critical business tools, there has been increased interest in techniques and methods to monitor the routing posture of networks. Incorrect routing or routing issues cause undesirable performance degradation, flapping and/or downtime. Monitoring routing in a network is achieved using Route analytics tools and techniques.

## References

- [1] RFC 3626
- [2] <http://rainer.baumann.info/public/tik262.pdf>
- [3] Jonne Zutt, Arjan J.C. van Gemund, Mathijs M. de Weerdt, and Cees Witteveen (2010). Dealing with Uncertainty in Operational Transport Planning (<http://www.st.ewi.tudelft.nl/~mathijs/publications/intinfra09.pdf>). In R.R. Negenborn and Z. Lukszo and H. Hellendoorn (Eds.) Intelligent Infrastructures, Ch. 14, pp. 355-382. Springer.
- [4] Matthew Caesar and Jennifer Rexford. BGP routing policies in ISP networks (<http://www.cs.princeton.edu/~jrex/papers/policies.pdf>). IEEE Network Magazine, special issue on Interdomain Routing, Nov/Dec 2005.
- [5] Neil Spring, Ratul Mahajan, and Thomas Anderson. Quantifying the Causes of Path Inflation (<http://www.cs.washington.edu/research/networking/rocketfuel/papers/sigcomm2003.pdf>). Proc. SIGCOMM 2003.
- [6] Ratul Mahajan, David Wetherall, and Thomas Anderson. Negotiation-Based Routing Between Neighboring ISPs (<http://research.microsoft.com/en-us/um/people/ratul/papers/nsdi2005-nexit.pdf>). Proc. NSDI 2005.
- [7] Ratul Mahajan, David Wetherall, and Thomas Anderson. Mutually Controlled Routing with Independent ISPs (<http://research.microsoft.com/en-us/um/people/ratul/papers/nsdi2007-wiser.pdf>). Proc. NSDI 2007.
- Ash, Gerald (1997). *Dynamic Routing in Telecommunication Networks*. McGraw-Hill. ISBN 0-07-006414-8.
- Doyle, Jeff and Carroll, Jennifer (2005). *Routing TCP/IP, Volume I, Second Ed.*. Cisco Press. ISBN 1-58705-202-4. Ciscopress ISBN 1-58705-202-4 (<http://www.ciscopress.com/title/1587052024>)
- Doyle, Jeff and Carroll, Jennifer (2001). *Routing TCP/IP, Volume II*. Cisco Press. ISBN 1-57870-089-2. Ciscopress ISBN 1-57870-089-2 (<http://www.ciscopress.com/title/1578700892>)
- Huitema, Christian (2000). *Routing in the Internet, Second Ed.*. Prentice-Hall. ISBN 0-321-22735-2.
- Kurose, James E. and Ross, Keith W. (2004). *Computer Networking, Third Ed.*. Benjamin/Cummings. ISBN 0-321-22735-2.
- Medhi, Deepankar and Ramasamy, Karthikeyan (2007). *Network Routing: Algorithms, Protocols, and Architectures*. Morgan Kaufmann. ISBN 0-12-088588-3.

## External links

- Count-To-Infinity Problem (<http://wiki.uni.lu/secan-lab/Count-To-Infinity+Problem.html>)
- "Stability Features" (<http://www.lehre.dhbw-stuttgart.de/~schulte/htme/55024.htm#HDR3>) are ways of avoiding the "count to infinity" problem.
- Cisco IT Case Studies ([http://www.cisco.com/web/about/ciscoitatwork/case\\_studies/routing.html](http://www.cisco.com/web/about/ciscoitatwork/case_studies/routing.html)) about Routing and Switching
- good example at event-helix ([http://www.eventhelix.com/Realtimemantra/Networking/ip\\_routing.htm](http://www.eventhelix.com/Realtimemantra/Networking/ip_routing.htm))

# Static routing

---

Static routing is a concept describing one way of configuring path selection of routers in computer networks. It is the type of routing characterized by the absence of communication between routers regarding the current topology of the network.<sup>[1]</sup> This is achieved by manually adding routes to the routing table. The opposite of static routing is dynamic routing, sometimes also referred to as *adaptive routing*.

In these systems, routes through a data network are described by fixed paths (statically). These routes are usually entered into the router by the system administrator. An entire network can be configured using static routes, but this type of configuration is not fault tolerant. When there is a change in the network or a failure occurs between two statically defined nodes, traffic will not be rerouted. This means that anything that wishes to take an affected path will either have to wait for the failure to be repaired or the static route to be updated by the administrator before restarting its journey. Most requests will time out (ultimately failing) before these repairs can be made. There are, however, times when static routes can improve the performance of a network. Some of these include stub networks and default routes.

## Example

To configure a static route to network 10.10.20.0/24, pointing to a next-hop router with the IP address of 192.168.100.1, type: (Note that this example is written in the Cisco IOS command line syntax and will only work on certain Cisco routers<sup>[2]</sup>)

```
ip route 10.10.20.0 255.255.255.0 192.168.100.1
```

Destination network	10.10.20.0
subnet	255.255.255.0
next-hop	192.168.100.1

The other option is to define a static route with reference to the outgoing interface which is connected to the next hop towards the destination network.

```
ip route 10.10.20.0 255.255.255.0 Serial 0/0
```

Destination network	10.10.20.0
subnet	255.255.255.0
next-hop	Serial interface 0/0 (local exit)

## References

- [1] TCP/IP Tutorial and Technical Overview (IBM RedBooks Series) (<http://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf>)  
[2] Cisco IOS Command Reference: ip route ([http://www.cisco.com/en/US/docs/ios/12\\_3t/ip\\_route/command/reference/ip2\\_i2gt.html#wp1106404](http://www.cisco.com/en/US/docs/ios/12_3t/ip_route/command/reference/ip2_i2gt.html#wp1106404))

# Link-state routing protocol

A **link-state routing protocol** is one of the two main classes of routing protocols used in packet switching networks for computer communications (the other is the distance-vector routing protocol). Examples of link-state routing protocols include OSPF and IS-IS.

The link-state protocol is performed by every *switching node* in the network (i.e. nodes that are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is that every node constructs a *map* of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical *path* from it to every possible destination in the network. The collection of best paths will then form the node's routing table.

This contrasts with distance-vector routing protocols, which work by having each node share its **routing table** with its neighbors. In a link-state protocol the only information passed between nodes is **connectivity related**.

Link state algorithms are sometimes characterized informally as each router 'telling the world about its neighbors'.

## History

What is believed to be the first adaptive routing network of computers, using link-state routing as its heart, was designed and implemented during 1976-77 by a team from Plessey Radar led by Bernard J Harris; the project was for "Wavell" - a system of computer command and control for the British Army.

The first link-state routing concept was published in 1979 by John M. McQuillan<sup>[1][2]</sup> (then at Bolt, Beranek and Newman) as a mechanism that would calculate routes more quickly when network conditions changed, and thus lead to more stable routing.

Later work at BBN Technologies showed how to use the link-state technique in a hierarchical system, i.e. one in which the network was divided into areas, so that each switching node does not need a map of the entire network, only the area(s) in which it is included.

The technique was later adapted for use in the contemporary link-state routing protocols IS-IS and OSPF. Cisco literature refers to EIGRP as a "hybrid" protocol, despite the fact it distributes routing tables instead of topology maps. However, it does synchronize routing tables at start up as OSPF does, and sends specific updates only when topology changes occur.

In 2004 Radia Perlman proposed using link-state routing for Layer 2 frame forwarding with devices called Routing Bridges or Rbridges. The Internet Engineering Task Force has standardized the TRILL protocol to accomplish this.

More recently, this hierarchical technique was applied to wireless mesh networks using the optimized link state routing protocol. Where a connection can have varying quality, the quality of a connection can be used to select better connections. This is used in some routing protocols that use radio frequency transmission.

In 2012 the IEEE completed and approved the standardization of the use of IS-IS to control Ethernet forwarding with IEEE 802.1aq Shortest Path Bridging (SPB).

## Distributing maps

This description covers only the simplest configuration; i.e. one with no areas, so that all nodes do have a map of the entire network. The hierarchical case is somewhat more complex; see the various protocol specifications.

As previously mentioned, the first main stage in the link-state algorithm is to give a map of the network to every node. This is done with several simple subsidiary steps.

### Determining the neighbors of each node

First, each node needs to determine what other ports it is connected to, over fully working links; it does this using a simple *reachability protocol* which it runs separately with each of its directly connected neighbors.

### Distributing the information for the map

Next, each node periodically and in case of connectivity changes makes up a short message, the link-state advertisement, which:

- Identifies the node which is producing it.
- Identifies all the other nodes (either routers or networks) to which it is directly connected.
- Includes a *sequence number*, which increases every time the source node makes up a new version of the message.

This message is then *flooded* throughout the network. As a necessary precursor, each node in the network remembers, for every other node in the network, the sequence number of the last link-state message which it received from that node. With that in hand, the method used is simple.

Starting with the node which originally produced the message, it sends a copy to all of its neighbors. When a link-state advertisement is received at a node, the node looks up the sequence number it has stored for the source of that link-state message. If this message is newer (i.e. has a higher sequence number), it is saved, and a copy is sent in turn to each of that node's neighbors.

This procedure rapidly gets a copy of the latest version of each node's link-state advertisement to every node in the network.

Networks running link state algorithms can also be segmented into hierarchies which limit the scope of route changes. These features mean that link state algorithms scale better to larger networks.

### Creating the map

Finally, with the complete set of link-state advertisements (one from each node in the network) in hand, it is obviously easy to produce the graph for the map of the network.

The algorithm simply iterates over the collection of link-state advertisements; for each one, it makes links on the map of the network, from the node which sent that message, to all the nodes which that message indicates are neighbors of the sending node.

No link is considered to have been correctly reported unless the two ends agree; i.e. if one node reports that it is connected to another, but the other node does not report that it is connected to the first, there is a problem, and the link is not included on the map.

## Notes about this stage

The link-state message giving information about the neighbors is recomputed, and then flooded throughout the network, whenever there is a change in the connectivity between the node and its neighbors, e.g. when a link fails. Any such change will be detected by the reachability protocol which each node runs with its neighbors.

## Calculating the routing table

As initially mentioned, the second main stage in the link-state algorithm is to produce routing tables, by inspecting the maps. This is again done with several steps.

### Calculating the shortest paths

Each node independently runs an algorithm over the map to determine the shortest path from itself to every other node in the network; generally some variant of Dijkstra's algorithm is used. This is based around a link cost across each path which includes available bandwidth among other things.

Basically, a node maintains two data structures: a tree containing nodes which are "done", and a list of *candidates*. The algorithm starts with both structures empty; it then adds to the first one the node itself. The variant of a Greedy Algorithm then repetitively does the following:

- All neighbour nodes which are directly connected to the node are just added to the tree (excepting any nodes which are already in either the tree or the candidate list). The rest are added to the second (candidate) list.
- Each node in the candidate list is compared to each of the nodes already in the tree. The candidate node which is closest to any of the nodes already in the tree is itself moved into the tree and attached to the appropriate neighbor node. When a node is moved from the candidate list into the tree, it is removed from the candidate list and is not considered in subsequent iterations of the algorithm.

The above two steps are repeated as long as there aren't any nodes left in the candidate list. (When there are none, all the nodes in the network will have been added to the tree.) This procedure ends with the tree containing all the nodes in the network, with the node on which the algorithm is running as the *root* of the tree. The shortest path from that node to any other node is indicated by the list of nodes one traverses to get from the root of the tree, to the desired node in the tree.

### Filling the routing table

With the shortest paths in hand, filling in the routing table is trivial.

For any given destination node, the best path for that destination is the node which is the first step from the root node, down the branch in the shortest-path tree which leads toward the desired destination node.

To create the routing table, it is only necessary to walk the tree, remembering the identity of the node at the head of each branch, and filling in the routing table entry for each node one comes across with that identity.

### Optimizations to the algorithm

The algorithm described above was made as simple as possible, to aid in ease of understanding. In practice, there are a number of optimizations which are used.

Most importantly, whenever a change in the connectivity map happens, it is necessary to recompute the shortest-path tree, and then recreate the routing table. Work by BBN Technologies discovered how to recompute only that part of the tree which could have been affected by a given change in the map.

Also, the routing table would normally be filled in as the shortest-path tree is computed, instead of making it a separate operation.

## Failure modes

If all the nodes are not working from **exactly** the same map, *routing loops* can form. (These are situations in which, in the simplest form, two neighboring nodes each think the other is the best path to a given destination. Any packet headed to that destination arriving at either node will loop between the two, hence the name. Routing loops involving more than two nodes are also possible.)

The reason is fairly simple: since each node computes its shortest-path tree and its routing table without interacting in any way with any other nodes, then if two nodes start with different maps, it is easy to have scenarios in which routing loops are created.

## The Optimized Link State Routing Protocol for Mobile ad-hoc Networks

A link-state routing protocol - optimized for mobile ad-hoc networks, which can also be used on other wireless ad-hoc networks - is the *Optimized Link State Routing Protocol* (OLSR).<sup>[3]</sup> OLSR is proactive, it uses Hello and Topology Control (TC) messages to discover and disseminate link state information into the mobile ad-hoc network. Using Hello messages each node discovers 2-hop neighbor information and elects a set of *multipoint relays* (MPRs). MPRs makes OLSR unique from other link state routing protocols. Individual nodes use the topology information to compute next hop paths regard to all nodes in the network utilising shortest hop forwarding paths.

## References

- [1] John M. McQuillan, Isaac Richer and Eric C. Rosen, *ARPANet Routing Algorithm Improvements*, BBN Report No. 3803, Cambridge, April 1978
- [2] John M. McQuillan, Isaac Richer and Eric C. Rosen, *The New Routing Algorithm for the ARPANet*, IEEE Trans. on Comm., 28(5), pp. 711–719, 1980
- [3] RFC 3626
  - Josh Seeger and Atul Khanna, *Reducing Routing Overhead in a Growing DDN*, MILCOMM '86, IEEE, 1986
  - Radia Perlman "Rbridges: Transparent Routing" ([http://www.ieee-infocom.org/2004/Papers/26\\_1.PDF](http://www.ieee-infocom.org/2004/Papers/26_1.PDF)), Infocom 2004.

## Further reading

- Section "Link-State Versus Distance Vector" ([http://docwiki.cisco.com/wiki/Routing\\_Basics#Link-State\\_Versus\\_Distance\\_Vector](http://docwiki.cisco.com/wiki/Routing_Basics#Link-State_Versus_Distance_Vector)) in the Chapter "Routing Basics" in the Cisco "Internetworking Technology Handbook"

# Open Shortest Path First

**Open Shortest Path First (OSPF)** is an adaptive routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4.<sup>[1]</sup> The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).<sup>[2]</sup>

OSPF is perhaps the most widely used interior gateway protocol (IGP) in large enterprise networks. IS-IS, another link-state dynamic routing protocol, is more common in large service provider networks. The most widely used exterior gateway protocol is the Border Gateway Protocol (BGP), the principal routing protocol between autonomous systems on the Internet.

## Overview

OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain (autonomous system). It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets. OSPF was designed to support variable-length subnet masking (VLSM) or Classless Inter-Domain Routing (CIDR) addressing models.

OSPF detects changes in the topology, such as link failures, very quickly and converges on a new loop-free routing structure within seconds. It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a shortest path first algorithm.

The **link-state** information is maintained on each router as a link-state database (LSDB) which is a tree-image of the entire network topology. Identical copies of the LSDB are periodically updated through flooding on all OSPF routers.

The OSPF routing policies to construct a route table are governed by link cost factors (*external metrics*) associated with each routing interface. Cost factors may be the distance of a router (round-trip time), network throughput of a link, or link availability and reliability, expressed as simple unitless numbers. This provides a dynamic process of traffic load balancing between routes of equal cost.

An OSPF network may be structured, or subdivided, into routing *areas* to simplify administration and optimize traffic and resource utilization. Areas are identified by 32-bit numbers, expressed either simply in decimal, or often in octet-based dot-decimal notation, familiar from IPv4 address notation.

By convention, area 0 (zero) or 0.0.0.0 represents the core or *backbone* region of an OSPF network. The identifications of other areas may be chosen at will; often, administrators select the IP address of a main router in an area as the area's identification. Each additional area must have a direct or virtual connection to the backbone OSPF area. Such connections are maintained by an interconnecting router, known as *area border router* (ABR). An ABR maintains separate link state databases for each area it serves and maintains summarized routes for all areas in the network.

OSPF does not use a TCP/IP transport protocol (UDP, TCP), but is encapsulated directly in IP datagrams with protocol number 89. This is in contrast to other routing protocols, such as the Routing Information Protocol (RIP), or the Border Gateway Protocol (BGP). OSPF handles its own error detection and correction functions.

OSPF uses multicast addressing for route flooding on a broadcast network link. For non-broadcast networks special provisions for configuration facilitate neighbor discovery.<sup>[1]</sup> OSPF multicast IP packets never traverse IP routers, they never travel more than one hop. OSPF reserves the multicast addresses 224.0.0.5 for IPv4 or FF02::5 for IPv6 (all SPF/link state routers, also known as AllSPFRouters) and 224.0.0.6 for IPv4 or FF02::6 for IPv6 (all Designated Routers, AllDRouters), as specified in RFC 2328<sup>[3]</sup> and RFC 5340.<sup>[4]</sup>

For routing multicast IP traffic, OSPF supports the Multicast Open Shortest Path First protocol (MOSPF) as defined in RFC 1584.<sup>[5]</sup> Neither Cisco nor Juniper Networks include MOSPF in their OSPF implementations. PIM (Protocol Independent Multicast) in conjunction with OSPF or other IGPs, (Interior Gateway Protocol), is widely deployed.

The OSPF protocol, when running on IPv4, can operate securely between routers, optionally using a variety of authentication methods to allow only trusted routers to participate in routing. OSPFv3, running on IPv6, no longer supports protocol-internal authentication. Instead, it relies on IPv6 protocol security (IPsec).

OSPF version 3 introduces modifications to the IPv4 implementation of the protocol.<sup>[2]</sup> Except for virtual links, all neighbor exchanges use IPv6 link-local addressing exclusively. The IPv6 protocol runs per link, rather than based on the subnet. All IP prefix information has been removed from the link-state advertisements and from the *Hello* discovery packet making OSPFv3 essentially protocol-independent. Despite the expanded IP addressing to 128-bits in IPv6, area and router identifications are still based on 32-bit values.

## Neighbor relationships

Routers in the same broadcast domain or at each end of a point-to-point telecommunications link form *adjacencies* when they have detected each other. This detection occurs when a router identifies itself in a *hello* OSPF protocol packet. This is called a *two-way state* and is the most basic relationship. The routers in an Ethernet or frame relay network select a *designated router* (DR) and a *backup designated router* (BDR) which act as a hub to reduce traffic between routers. OSPF uses both unicast and multicast to send "hello packets" and link state updates.

As a link state routing protocol, OSPF establishes and maintains neighbor relationships in order to exchange routing updates with other routers. The neighbor relationship table is called an adjacency database in OSPF. Provided that OSPF is configured correctly, OSPF forms neighbor relationships only with the routers directly connected to it. In order to form a neighbor relationship between two routers, the interfaces used to form the relationship must be in the same area. An interface can only belong to a single area. (A neighbor state simulation<sup>[6]</sup> shows how neighbor state changes from Down to Full Adjacency progressively with exchanging Hello, DD, Request, Update, and Ack packets).

## Area types

An OSPF domain is divided into *areas* that are labeled with 32-bit area identifiers. The area identifiers are commonly, but not always, written in the dot-decimal notation of an IPv4 address. However, they are *not* IP addresses and may duplicate, without conflict, any IPv4 address. The area identifiers for IPv6 implementations of OSPF (OSPFv3) also use 32-bit identifiers written in the same notation. While most OSPF implementations will right-justify an area number written in a format other than dotted decimal format (e.g., area 1), it is wise to always use dotted-decimal formats. Most implementations expand area 1 to the area identifier 0.0.0.1, but some have been known to expand it as 1.0.0.0.

Areas are logical groupings of hosts and networks, including their routers having interfaces connected to any of the included networks. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Thus, the topology of an area is unknown outside of the area. This reduces the amount of routing traffic between parts of an autonomous system. (An ABR simulation<sup>[7]</sup> shows how an ABR lets areas know each others' network addresses by flooding Summary LSA.)

Several special area types are defined.

## Backbone area

The backbone area (also known as *area 0* or *area 0.0.0.0*) forms the core of an OSPF network. All other areas are connected to it, and inter-area routing happens via routers connected to the backbone area and to their own associated areas. It is the logical and physical structure for the 'OSPF domain' and is attached to all nonzero areas in the OSPF domain. Note that in OSPF the term Autonomous System Boundary Router (ASBR) is historic, in the sense that many OSPF domains can coexist in the same Internet-visible autonomous system, RFC1996 (ASGuidelines 1996, p. 25).<sup>[8]</sup>

The backbone area is responsible for distributing routing information between nonbackbone areas. The backbone must be contiguous, but it does not need to be physically contiguous; backbone connectivity can be established and maintained through the configuration of virtual links.

All OSPF areas must connect to the backbone area. This connection, however, can be through a virtual link. For example, assume area 0.0.0.1 has a physical connection to area 0.0.0.0. Further assume that area 0.0.0.2 has no direct connection to the backbone, but this area does have a connection to area 0.0.0.1. Area 0.0.0.2 can use a virtual link through the *transit area* 0.0.0.1 to reach the backbone. To be a transit area, an area has to have the *transit* attribute, so it cannot be stubby in any way.

## Stub area

A stub area is an area which does not receive route advertisements external to the autonomous system (AS) and routing from within the area is based entirely on a default route. A Stub Area simulation<sup>[9]</sup> shows how an ABR deletes type 4, 5 LSAs from internal routers, sends them a default route of 0.0.0.0 and turns itself into a default gateway. This reduces LSDB and routing table size for internal routers.

Modifications to the basic concept of stub areas exist in the *not-so-stubby* area (NSSA). In addition, several other proprietary variations have been implemented by systems vendors, such as the *totally stubby area* (TSA) and the *NSSA not so stubby area*, both an extension in Cisco Systems routing equipment.

### Not-so-stubby area

A *not-so-stubby area* (NSSA) is a type of stub area that can import autonomous system external routes and send them to other areas, but still cannot receive AS-external routes from other areas. NSSA is an extension of the stub area feature that allows the injection of external routes in a limited fashion into the stub area. A case study simulates<sup>[10]</sup> an NSSA getting around the Stub Area problem of not being able to import external addresses. It visualizes the following activities: the ASBR imports external addresses with a type 7 LSA, the ABR converts a type 7 LSA to type 5 and floods it to other areas, the ABR acts as an "ASBR" for other areas. The ABR's do not take type 5 LSA's and then convert to type 7 LSA's for the area.

### Proprietary extensions

Several vendors (Cisco, Juniper, Alcatel-Lucent, Huawei, Quagga), now implement the below two extensions to stub and NSSA area and although not covered by RFC they are considered by many to be standard features in OSPF implementations.

#### Totally stubby area

A *totally stubby area* is similar to a stub area. However, this area does not allow *summary* routes in addition to not having *external* routes, that is, *inter-area* (IA) routes are not summarized into totally stubby areas. The only way for traffic to get routed outside of the area is a default route which is the only Type-3 LSA advertised into the area. When there is only one route out of the area, fewer routing decisions have to be made by the route processor, which lowers system resource utilization.

Occasionally, it is said that a TSA can have only one ABR.<sup>[11]</sup>

### NSSA totally stubby area

An addition to the standard functionality of an NSSA, the *totally stubby* NSSA is an NSSA that takes on the attributes of a TSA, meaning that type 3 and 4 summary routes are not flooded into this type of area. It is also possible to declare an area both totally stubby and not-so-stubby, which means that the area will receive only the default route from area 0.0.0.0, but can also contain an autonomous system boundary router (ASBR) that accepts external routing information and injects it into the local area, and from the local area into area 0.0.0.0.

Redistribution into an NSSA area creates a special type of LSA known as TYPE 7, which can exist only in an NSSA area. An NSSA ASBR generates this LSA, and an NSSA ABR router translates it into type 5 LSA which gets propagated into the OSPF domain.

A newly acquired subsidiary is one example of where it might be suitable for an area to be simultaneously not-so-stubby and totally stubby if the practical place to put an ASBR is on the edge of a totally stubby area. In such a case, the ASBR does send externals into the totally stubby area, and they are available to OSPF speakers within that area. In Cisco's implementation, the external routes can be summarized before injecting them into the totally stubby area. In general, the ASBR should not advertise default into the TSA-NSSA, although this can work with extremely careful design and operation, for the limited special cases in which such an advertisement makes sense.

By declaring the totally stubby area as NSSA, no external routes from the backbone, except the default route, enter the area being discussed. The externals do reach area 0.0.0.0 via the TSA-NSSA, but no routes other than the default route enter the TSA-NSSA. Routers in the TSA-NSSA send all traffic to the ABR, except to routes advertised by the ASBR.

### Transit area

A transit area is an area with two or more OSPF border routers and is used to pass network traffic from one adjacent area to another. The transit area does not originate this traffic and is not the destination of such traffic.

### Path preference

OSPF uses *path cost* as its basic routing metric, which was defined by the standard not to equate to any standard value such as speed, so the network designer could pick a metric important to the design. In practice, it is determined by the speed (bandwidth) of the interface addressing the given route, although that tends to need network-specific scaling factors now that links faster than 100 Mbit/s are common. Cisco uses a metric like  $10^8/\text{bandwidth}$  (the base value,  $10^8$  by default, can be adjusted). So, a 100Mbit/s link will have a cost of 1, a 10Mbit/s a cost of 10 and so on. But for links faster than 100Mbit/s, the cost would be <1.

Metrics, however, are only directly comparable when of the same type. Four types of metrics are recognized. An intra-area route is always preferred to an External route regardless of metric. In decreasing preference, these types are:

1. Intra-area
2. Inter-area
3. External Type 1, which includes both the external path cost and the sum of internal path costs to the ASBR that advertises the route,
4. External Type 2, the value of which is solely that of the external path cost

## Traffic engineering

OSPF-TE is an extension to OSPF extending the expressivity to allow for traffic engineering and use on non-IP networks (RFC 3630).<sup>[12]</sup> More information about the topology can be exchanged using opaque LSA carrying type-length-value elements. These extensions allow OSPF-TE to run completely out of band of the data plane network. This means that it can also be used on non-IP networks, such as optical networks.

OSPF-TE is used in GMPLS networks as a means to describe the topology over which GMPLS paths can be established. GMPLS uses its own path setup and forwarding protocols, once it has the full network map.

In the Resource Reservation Protocol (RSVP), OSPF-TE is used for recording and flooding RSVP signaled bandwidth reservations for Label switched paths within the link-state database.

## Other extensions

RFC 3717 documents work in optical routing for IP, based on "constraint-based" extensions to OSPF and IS-IS.<sup>[13]</sup>

## OSPF router types

OSPF defines the following router types:

- Area border router (ABR)
- Autonomous system boundary router (ASBR)
- Internal router (IR)
- Backbone router (BR)

The router type is an attribute of an OSPF process. A given physical router may have one or more OSPF processes. For example, a router that is connected to more than one area, and which receives routes from a BGP process connected to another AS, is both an area border router and an autonomous system boundary router.

Each router has an identifier, customarily written in the dotted decimal format (e.g., 1.2.3.4) of an IP address. This identifier must be established in every OSPF instance. If not explicitly configured, the highest logical IP address will be duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network, and often isn't to avoid confusion.

These router types should not be confused with the terms *designated router (DR)*, or *backup designated router (BDR)*, which are attributes of a router interface, not the router itself.

### Area border router

An area border router (ABR) is a router that connects one or more areas to the main backbone network. It is considered a member of all areas it is connected to. An ABR keeps multiple copies of the link-state database in memory, one for each area to which that router is connected.

### Autonomous system boundary router

An autonomous system boundary router (ASBR) is a router that is connected to more than one Routing protocol and that exchanges routing information with routers in other protocols. ASBRs typically also run an exterior routing protocol (e.g., BGP), or use static routes, or both. An ASBR is used to distribute routes received from other, external ASs throughout its own autonomous system. (An interactive ASBR simulation<sup>[14]</sup> shows how an ASBR creates External LSA for external addresses and floods them to all areas via ABR.) Routers in other areas use ABR as next hop to access external addresses. Then ABR forwards packets to the ASBR that announces the external addresses.

## Internal router

An internal router is a router that has OSPF neighbor relationships with interfaces in the same area. An internal router has all its interfaces in a single area.

## Backbone router

Backbone routers are all routers that are connected to the OSPF backbone, irrespective of whether they are also area border routers or internal routers of the backbone area. An area border router is always a backbone router, since all areas must be either directly connected to the backbone or connected to the backbone via a virtual link (spanning across another area to get to the backbone).

## Designated router

A *designated router* (DR) is the router interface elected among all routers on a particular multiaccess network segment, generally assumed to be broadcast multiaccess. A DR Election Simulation<sup>[15]</sup> visualizes the basic neighbor discovery process (Hello), flooding (224.0.0.6), DR election (priority, RID). Special techniques, often vendor-dependent, may be needed to support the DR function on nonbroadcast multiaccess (NBMA) media. It is usually wise to configure the individual virtual circuits of a NBMA subnet as individual point-to-point lines; the techniques used are implementation-dependent.

Do not confuse the DR with an OSPF router type. A given physical router can have some interfaces that are designated (DR), others that are backup designated (BDR), and others that are non-designated. If no router is DR or BDR on a given subnet, the DR is first elected, and then a second election is held if there is more than one BDR.<sup>[16]</sup> (A DR Election Detail Simulation<sup>[17]</sup> shows a step-by-step DR election example: How neighbor list, neighbor state, DR, and BDR are changed when receiving Hello) The DR is elected based on the following default criteria:

- If the priority setting on an OSPF router is set to 0, that means it can NEVER become a DR or BDR (Backup Designated Router).
- When a DR fails and the BDR takes over, there is another election to see who becomes the replacement BDR.
- The router sending the Hello packets with the highest priority wins the election.
- If two or more routers tie with the highest priority setting, the router sending the Hello with the highest RID (Router ID) wins. NOTE: a RID is the highest logical (loopback) IP address configured on a router, if no logical/loopback IP address is set then the Router uses the highest IP address configured on its active interfaces. (e.g. 192.168.0.1 would be higher than 10.1.1.2).
- Usually the router with the second highest priority number becomes the BDR.
- The priority values range between 0 - 255,<sup>[18]</sup> with a higher value increasing its chances of becoming DR or BDR.
- IF a HIGHER priority OSPF router comes online AFTER the election has taken place, it will not become DR or BDR until (at least) the DR and BDR fail.
- If the current DR 'goes down' the current BDR becomes the new DR and a new election takes place to find another BDR. If the new DR then 'goes down' and the original DR is now available, still previously chosen BDR will become DR.

DR's exist for the purpose of reducing network traffic by providing a source for routing updates. The DR maintains a complete topology table of the network and sends the updates to the other routers via multicast. All routers in a multi-access network segment will form a slave/master relationship with the DR. They will form adjacencies with the DR and BDR only. Every time a router sends an update, it sends it to the DR and BDR on the multicast address 224.0.0.6. The DR will then send the update out to all other routers in the area, to the multicast address 224.0.0.5. This way all the routers do not have to constantly update each other, and can rather get all their updates from a single source. The use of multicasting further reduces the network load. DRs and BDRs are always setup/elected on OSPF broadcast networks. DR's can also be elected on NBMA (Non-Broadcast Multi-Access) networks such as Frame Relay or ATM. DRs or BDRs are not elected on point-to-point links (such as a point-to-point WAN connection)

because the two routers on either sides of the link must become fully adjacent and the bandwidth between them cannot be further optimized. DR LSDB Synch Simulation [19] shows how DR and non-DR routers evolve from 2-way to full adjacency relationships by exchanging DD, Request, and Update.

## **Backup designated router**

A *backup designated router* (BDR) is a router that becomes the designated router if the current designated router has a problem or fails. The BDR is the OSPF router with second highest priority at the time of the last election.

## OSPF v3 Packet Formats

The "Main OSPF Packet Header" is the same for all 5 types of packets (with exception of the Type field) whereas the following sub-headers will vary from type to type and are shown below the Main OSPF Packet Header.

## The Main OSPF Packet Header

As per Appendix A.3 of RFC 5340 (OSPFv3 for IPv6) there are 5 OSPF Packet formats as follows:

Type	Description
1	Hello
2	Database Description
3	Link State Request
4	Link State Update
5	Link State Acknowledgement

The five different formats for each "Type" of OSPF v3 packet are listed below:

## Type 1: The Hello Packet

## Type 2: The Database Description Packet

## Type 3: The OSPF Link State Request Packet

### Type 4: The OSPF Link State Update Packet

Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																
0	0	3 {Ver}				4 {Type}				Packet Length																																							
4	32	Router ID																																															
8	64	Area ID																																															
12	96	Checksum																Instance ID				0																											
16	128	# LSAs																																															
20	160	LSAs																																															
24	192																																																
28	224																																																
32	256																																																
36	288																																																
~	~	...																																															

### Type 5: The OSPF Link State Acknowledgement Packet

Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																
0	0	3 {Ver}				5 {Type}				Packet Length																																							
4	32	Router ID																																															
8	64	Area ID																																															
12	96	Checksum																Instance ID				0																											
16	128	An LSA Header (Shown below)																																															
20	160																																																
24	192																																																
28	224																																																
32	256																																																
~	~	...																																															

### The OSPFv3 (24 Bit) Options Field

This "Options Field" is used in OSPF Hello packets, Database Description packets, and certain LSAs (router-LSAs, network-LSAs, inter-area-router-LSAs, and link-LSAs).

(Note: Previous OSPF versions { v1 & v2 } DO NOT support all of the options/fields listed here.)

Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
																	*	*	DC	R	N	x	E	V6

Explanation of the bits in the Options field:

There are currently only 7-bits assigned.

V6-bit: "V6" stands for IP[v6] routing calculations are to be used.

E-bit: "E" stands for [E]xternal as in AS-External-LSA flooding as specified in OSPFv2.

x-bit: This is currently deprecated. It was previously used by MOSPF.

- N-bit: "N" stands for [N]SSA (Not So Stubby Area) and used for routers which are attached to NSSA networks.
  - R-bit: "R" stands for [R]outer and specifies whether the router is Active or not.
  - DC-bit: "DC" stands for [D]emand [C]ircuits and is specified in RFC 1793.
  - \*-bits: These two bits are reserved for migration of OSPFv2 protocol extensions.
- The remaining 16-bits have yet to be assigned.

## OSPF in broadcast and non-broadcast networks

In broadcast multiple-access networks, neighbor adjacency is formed dynamically using multicast hello packets to 224.0.0.5. A DR and BDR are elected normally, and function normally.

For non-broadcast multiple-access networks (NBMA), RFC 2328 defined the following two official modes for OSPF:

- nonbroadcast
- point-to-multipoint

Cisco has defined the following three additional modes for OSPF in NBMA topologies:

- point-to-multipoint nonbroadcast
- broadcast
- point-to-point

## Implementations

- BIRD implements both OSPFv2 and OSPFv3
- GNU Zebra, a GPL routing suite for Unix-like systems supporting OSPF
- Netware implements OSPF in its Multi Protocol Routing module.
- OpenBSD includes an OpenOSPF implementation within the OpenBGPD protocol.
- Quagga, a fork of GNU Zebra for Unix-like systems
- XORP, a routing suite implementing RFC2328 (OSPFv2) and RFC2740 (OSPFv3) for both IPv4 and IPv6
- Windows NT 4.0 Server, Windows 2000 Server and Windows Server 2003 implement OSPFv2 in the Routing and Remote Access Service, although the functionality was removed in Windows Server 2008.

## Applications

OSPF was the first widely deployed routing protocol that could converge a network in the low seconds, and guarantee loop-free paths. It has many features that allow the imposition of policies about the propagation of routes that it may be appropriate to keep local, for load sharing, and for selective route importing more than IS-IS. IS-IS, in contrast, can be tuned for lower overhead in a stable network, the sort more common in ISP than enterprise networks. There are some historical accidents that made IS-IS the preferred IGP for ISPs, but ISP's today may well choose to use the features of the now-efficient implementations of OSPF,<sup>[20]</sup> after first considering the pros and cons of IS-IS in service provider environments.<sup>[21]</sup>

As mentioned, OSPF can provide better load-sharing on external links than other IGPs. When the default route to an ISP is injected into OSPF from multiple ASBRs as a Type I external route and the same external cost specified, other routers will go to the ASBR with the least path cost from its location. This can be tuned further by adjusting the external cost.

In contrast, if the default route from different ISPs is injected with different external costs, as a Type II external route, the lower-cost default becomes the primary exit and the higher-cost becomes the backup only.

The only real limiting factor that may compel major ISPs to select IS-IS over OSPF is if they have a network with more than 850 routers. There is mention of an OSPF network with over 1000 routers,<sup>[22]</sup> but that is quite uncommon and the network must be specifically designed to minimize overhead to achieve stable operation.

## References

- [1] Moy, J. (April 1998). [RFC 2328 "OSPF Version 2"]. The Internet Society. OSPFv2. RFC 2328. Retrieved 2007-09-28.
- [2] Colton, R.; D. Ferguson, J Moy, A. Lindem (July 2008). [RFC 5340 "OSPF for IPv6"]. The Internet Society. OSPFv3. RFC 5340. Retrieved 2008-07-23.
- [3] "RFC 2328 - OSPF Version 2" (<http://tools.ietf.org/html/rfc2328#page-185>). Tools.ietf.org. 1998-04-02. . Retrieved 2011-11-30.
- [4] "RFC 5340 - OSPF for IPv6" (<http://tools.ietf.org/html/rfc5340#page-57>). Tools.ietf.org. . Retrieved 2011-11-30.
- [5] RFC 1584, *Multicast Extensions to OSPF*, J. Moy, The Internet Society (March 1994)
- [6] <http://www.youtube.com/watch?v=ajCwMMXGHVc>
- [7] <http://www.visualland.net/view.php?cid=931>
- [8] Hawkinson, J; T. Bates (March 1996). "Guidelines for creation, selection, and registration of an Autonomous System" (<http://tools.ietf.org/html/rfc1930>). Internet Engineering Task Force. ASguidelines. . Retrieved 2007-09-28.
- [9] <http://www.visualland.net/view.php?cid=760>
- [10] <http://www.visualland.net/view.php?cid=761>
- [11] "Stub Area Design Golden Rules" (<http://www.groupstudy.com/bookstore/samples/thomas/>). Groupstudy.com. . Retrieved 2011-11-30.. Note: This is not necessarily true. If there are multiple ABRs, as might be required for high availability, routers interior to the TSA will send non-intra-area traffic to the ABR with the lowest intra-area metric (the "closest" ABR) but that requires special configuration.
- [12] Katz, D; D. Yeung (September 2003). [RFC 3630 "Traffic Engineering (TE) Extensions to OSPF Version 2"]. The Internet Society. OSPF-TEextensions. RFC 3630. Retrieved 2007-09-28.
- [13] Rajagopalan, B; J. Luciani & D. Awduche (March 2004). [RFC 3717 "IP over Optical Networks: A Framework"]. Internet Engineering Task Force. OSPFoverOptical. RFC 3717. Retrieved 2007-09-28.
- [14] <http://www.visualland.net/view.php?cid=927>
- [15] <http://www.visualland.net/view.php?cid=924>
- [16] RFC 2328, page 75
- [17] <http://www.visualland.net/view.php?cid=940>
- [18] [http://www.cisco.com/en/US/docs/ios/iproute\\_ospf/command/reference/iro\\_cr\\_book.pdf](http://www.cisco.com/en/US/docs/ios/iproute_ospf/command/reference/iro_cr_book.pdf)
- [19] <http://www.visualland.net/view.php?cid=941>
- [20] Berkowitz, Howard (1999). "OSPF Goodies for ISPs" (<http://www.nanog.org/meetings/nanog17/abstracts.php?pt=MTE0OSZuYW5vZzE3&nm=nanog17>). North American Network Operators Group NANOG 17. Montreal. OSPFforISPs.
- [21] Katz, Dave (2000). "OSPF and IS-IS: A Comparative Anatomy" (<http://www.nanog.org/meetings/nanog19/abstracts.php?pt=MTA4NCZuYW5vZzE5&nm=nanog19>). North American Network Operators Group NANOG 19. Albuquerque. OSPFvsISIS.
- [22] "CCIE, CCNA, CCNP and other Cisco Certifications" (<http://www.groupstudy.com/archives/cisco/200011/msg01985.html>). GroupStudy.com. . Retrieved 2011-11-30.

## Further reading

- Colton, Andrew. *OSPF for Cisco Routers*. Rocket Science Press. ISBN 978-0972286213.
- Doyle, Jeff; Carroll, Jennifer. *Routing TCP/IP* (<http://www.ciscopress.com/bookstore/product.asp?isbn=1587052024>). 1 (2nd ed.). Cisco Press. ISBN 978-1-58705-202-6.
- Moy, John T.. *OSPF: Anatomy of an Internet Routing Protocol*. Addison-Wesley. ISBN 978-0201634723.
- Parkhurst, William R.. *Cisco OSPF Command and Configuration Handbook*. ISBN 978-1-58705-071-8.
- "Configuring OSPF Authentication" (<http://www.netcordia.com/resources/tech-tips/configuring-ospf-authentication.asp>). *Tech Tips*. Netcordia. Retrieved 2009-09-10.
- Basu, Anindya; Riecke, Jon (2001). "Stability issues in OSPF routing". *Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*. SIGCOMM '01. pp. 225–236. doi:10.1145/383059.383077. ISBN 1-58113-411-8. CiteSeerX: 10.1.1.99.6393 (<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.99.6393>).

## External links

- IETF OSPF Working Group (<http://www.ietf.org/html.charters/ospf-charter.html>)
- OSPF Basics (<http://www.setup32.com/network-administration/networking/know-ospf.php>)
- Cisco OSPF ([http://www.cisco.com/en/US/tech/tk365/tk480/tsd\\_technology\\_support\\_sub-protocol\\_home.html](http://www.cisco.com/en/US/tech/tk365/tk480/tsd_technology_support_sub-protocol_home.html))
- Cisco OSPF Areas and Virtual Links ([http://www.cisco.com/en/US/tech/tk365/technologies\\_tech\\_note09186a0080094aaa.shtml](http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094aaa.shtml))
- Summary of OSPF v2 (<http://www.freesoft.org/CIE/Topics/89.htm>)
- OSPF and IS-IS: A Comparative Anatomy (<http://www.nanog.org/meetings/nanog19/presentations/katz.ppt>) by Dave Katz, Juniper
- IS-IS and OSPF difference discussion (<http://www.join.uni-muenster.de/Dokumente/drafts/draft-bhatia-manral-diff-isis-ospf-01.txt>) (Vishwas Manral, Manav bhatia and Yasuhiro Ohara)
- Data Communication Lectures of Manfred Lindner - Part OSPF Fundamentals ([http://www.ict.tuwien.ac.at/lva/384.081/infobase/L41-OSPF\\_Fundamentals\\_v4-5.pdf](http://www.ict.tuwien.ac.at/lva/384.081/infobase/L41-OSPF_Fundamentals_v4-5.pdf))
- Data Communication Lectures of Manfred Lindner - Part OSPF Areas ([http://www.ict.tuwien.ac.at/lva/384.081/infobase/L42-OSPF\\_Advanced\\_v4-4.pdf](http://www.ict.tuwien.ac.at/lva/384.081/infobase/L42-OSPF_Advanced_v4-4.pdf))
- Good comparison of IS-IS vs OSPF (<http://www.ecse.rpi.edu/Homepages/koushik/shivkuma-teaching/sp2002/ip2002-isis-ospf.pdf>)

## Routing Information Protocol

The **Routing Information Protocol (RIP)** is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

RIP implements the split horizon, route poisoning and holddown mechanisms to prevent incorrect routing information from being propagated. These are some of the stability features of RIP. It is also possible to use the so called RMTI<sup>[1]</sup> (**R**outing **I**nformation **P**rotocol with **M**etric-based **T**opology **I**nvestigation) algorithm to cope with the count-to-infinity problem. With its help, it is possible to detect every possible loop with a very small computation effort.

Originally each RIP router transmitted full updates every 30 seconds. In the early deployments, routing tables were small enough that the traffic was not significant. As networks grew in size, however, it became evident there could be a massive traffic burst every 30 seconds, even if the routers had been initialized at random times. It was thought, as a result of random initialization, the routing updates would spread out in time, but this was not true in practice. Sally Floyd and Van Jacobson showed in 1994<sup>[2]</sup> that, without slight randomization of the update timer, the timers synchronized over time. In most current networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS (the latter two being link-state routing protocols), and (without RMTI) a hop limit severely limits the size of network it can be used in. However, it is easy to configure, because RIP does not require any parameters on a router unlike other protocols (see here<sup>[3]</sup> for an animation of basic RIP simulation visualizing RIP configuration and exchanging of Request and Response to discover new routes).

RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.<sup>[4]</sup>

## Versions

There are three versions of the Routing Information Protocol: *RIPv1*, *RIPv2*, and *RIPng*.

### RIP version 1

The original specification of RIP, defined in RFC 1058,<sup>[5]</sup> uses classful routing. The periodic routing updates do not carry subnet information, lacking support for variable length subnet masks (VLSM). This limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size. There is also no support for router authentication, making RIP vulnerable to various attacks.

### RIP version 2

Due to the deficiencies of the original RIP specification, RIP version 2 (RIPv2) was developed in 1993<sup>[6]</sup> and last standardized in 1998.<sup>[7]</sup> It included the ability to carry subnet information, thus supporting Classless Inter-Domain Routing (CIDR). To maintain backward compatibility, the hop count limit of 15 remained. RIPv2 has facilities to fully interoperate with the earlier specification if all *Must Be Zero* protocol fields in the RIPv1 messages are properly specified. In addition, a *compatibility switch* feature<sup>[7]</sup> allows fine-grained interoperability adjustments.

In an effort to avoid unnecessary load on hosts that do not participate in routing, RIPv2 *multicasts* the entire routing table to all adjacent routers at the address 224.0.0.9, as opposed to RIPv1 which uses broadcast. Unicast addressing is still allowed for special applications.

(MD5) authentication for RIP was introduced in 1997.<sup>[8][9]</sup>

RIPv2 is Internet Standard STD56 (which is RFC 2453).

Route tags were also added in RIP version 2. This functionality allows for routes to be distinguished from internal routes to external redistributed routes from EGP protocols.

### RIPng

RIPng (RIP next generation), defined in RFC 2080,<sup>[10]</sup> is an extension of RIPv2 for support of IPv6, the next generation Internet Protocol. The main differences between RIPv2 and RIPng are:

- Support of IPv6 networking.
- While RIPv2 supports RIPv1 updates authentication, RIPng does not. IPv6 routers were, at the time, supposed to use IPsec for authentication.
- RIPv2 allows attaching arbitrary tags to routes, RIPng does not;
- RIPv2 encodes the next-hop into each route entries, RIPng requires specific encoding of the next hop for a set of route entries.

RIPng sends updates on UDP port 521 using the multicast group FF02::9.

## Limitations

- Without using RMTI, Hop count can not exceed 15, in the case that it exceeds this limitation, it will be considered invalid.
- Most RIP networks are flat. There is no concept of areas or boundaries in RIP networks.
- Variable Length Subnet Masks were not supported by RIP version 1.
- Without using RMTI, RIP has slow convergence and count to infinity problems.

## Implementations

- Cisco IOS, software used in Cisco routers (supports version 1, version 2 and RIPng)
- Cisco NX-OS software used in Cisco Nexus data center switches (supports RIPv1 and RIPv2)
- Junos software used in Juniper routers, switches, and firewalls (supports RIPv1 and RIPv2)
- routed,<sup>[11]</sup> included in most BSD Unix systems
- Routing and Remote Access, a Windows Server feature, contains RIP support
- Quagga, a free open source routing software suite based on GNU Zebra
- BIRD, a free open source routing software suite
- OpenBSD, includes a RIP implementation

## Similar protocols

- IGRP:** Cisco's proprietary Interior Gateway Routing Protocol (IGRP) was a somewhat more capable protocol than RIP. It belongs to the same basic family of distance-vector routing protocols. Cisco has ceased support and distribution of IGRP in their router software. It was replaced by the Enhanced Interior Gateway Routing Protocol (EIGRP) which is a completely new design. While EIGRP still uses a distance-vector model, it relates to IGRP only in using the same routing metrics. IGRP supports multiple metrics for each route, including bandwidth, delay, load, MTU, and reliability.

## References

- [1] "RMTI project" (<http://userp.uni-koblenz.de/~vnuml/rmti/>). .
- [2] The Synchronization of Periodic Routing Messages ([http://www.icir.org/floyd/papers/sync\\_94.pdf](http://www.icir.org/floyd/papers/sync_94.pdf)), S. Floyd & V. Jacobson, April 1994
- [3] <http://www.learningocean.com/view.php?cid=899&protocol=RIP&title=1.%20RIP%20Basic&ctype=1>
- [4] "Port Numbers" (<http://www.iana.org/assignments/port-numbers>) (plain text). The Internet Assigned Numbers Authority (IANA). 2008-05-22. . Retrieved 2008-05-25.
- [5] RFC 1058, *Routing Information Protocol*, C. Hendrik, The Internet Society (June 1988)
- [6] RFC 1388, *RIP Version 2 - Carrying Additional Information*, G. Malkin, The Internet Society (January 1993)
- [7] RFC 2453, *RIP Version 2*, G. Malkin, The Internet Society (November 1998)
- [8] RFC 2082, *RIP-2 MD5 Authentication*, F. Baker, R. Atkinson, The Internet Society (January 1997)
- [9] RFC 4822, *RIPv2 Cryptographic Authentication*, R. Atkinson, M. Fanto, The Internet Society (January 2007)
- [10] RFC 2080, *RIPng for IPv6*, G. Malkin, R. Minnear, The Internet Society (January 1997)
- [11] Man-page for "routed(8)" on FreeBSD, <http://www.freebsd.org/cgi/man.cgi?query=routed&sektion=8>

## Further reading

- Malkin, Gary Scott (2000). *RIP: An Intra-Domain Routing Protocol*. Addison-Wesley Longman. ISBN 0-201-43320-6.
- Edward A. Taft, *Gateway Information Protocol (revised)* (Xerox Parc, Palo Alto, May, 1979)
- *Xerox System Integration Standard - Internet Transport Protocols* (Xerox, Stamford, 1981)

## External links

- Interactive RIP simulation (<http://www.visualland.net/view.php?cid=899&protocol=RIP&title=1.RIPBasic&ctype=1>)

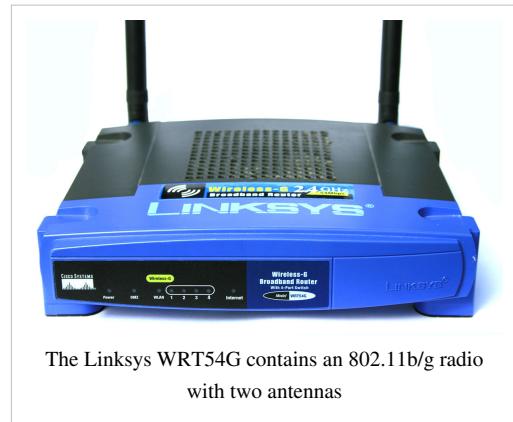
# IEEE 802.11

## IEEE 802.11

**IEEE 802.11** is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard **IEEE 802.11-2012** has had subsequent amendments. These standards provide the basis for wireless network products using the Wi-Fi brand.

### General description

The 802.11 family consists of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. 802.11n is a new multi-streaming modulation technique. Other standards in the family (c-f, h, j) are service amendments and extensions or corrections to the previous specifications.



802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones and Bluetooth devices. 802.11b and 802.11g control their interference and susceptibility to interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signaling methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap - see list of WLAN channels. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment.

The segment of the radio frequency spectrum used by 802.11 varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six of 802.11b and 802.11g fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.<sup>[1]</sup>

### History

802.11 technology has its origins in a 1985 ruling by the U.S. Federal Communications Commission that released the ISM band for unlicensed use.<sup>[2][3]</sup>

In 1991 NCR Corporation/AT&T (now Alcatel-Lucent and LSI Corporation) invented the precursor to 802.11 in Nieuwegein, The Netherlands. The inventors initially intended to use the technology for cashier systems; the first wireless products were brought on the market under the name WaveLAN with raw data rates of 1 Mbit/s and 2 Mbit/s.

Vic Hayes, who held the chair of IEEE 802.11 for 10 years and has been called the "father of Wi-Fi" was involved in designing the initial 802.11b and 802.11a standards within the IEEE.

In 1999, the Wi-Fi Alliance was formed as a trade association to hold the Wi-Fi trademark under which most products are sold.<sup>[4]</sup>

## Protocols

802.11 network standards										
802.11 protocol	Release [5]	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s) <sup>[6]</sup>	Allowable MIMO streams	Modulation	Approximate indoor range		Approximate outdoor range	
							(m)	(ft)	(m)	(ft)
—	Jun 1997	2.4	20	1, 2	1	DSSS, FHSS	20	unknown operator: u'strong'	100	unknown operator: u'strong'
a	Sep 1999	5 3.7 <sup>[A]</sup>	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	unknown operator: u'strong'	120	unknown operator: u'strong'
							—	—	5000	unknown operator: u'strong' <sup>[A]</sup>
b	Sep 1999	2.4	20	1, 2, 5.5, 11	1	DSSS	35	unknown operator: u'strong'	140	unknown operator: u'strong'
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	unknown operator: u'strong'	140	unknown operator: u'strong'
n	Oct 2009	2.4/5	20 40	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 <sup>[B]</sup>	4	OFDM	70	unknown operator: u'strong'	250	unknown operator: u'strong' <sup>[7]</sup>
				15, 30, 45, 60, 90, 120, 135, 150 <sup>[B]</sup>			70	unknown operator: u'strong'	250	unknown operator: u'strong' <sup>[7]</sup>
ac (DRAFT)	Nov. 2011	5	20	up to 87.6 <sup>[8]</sup>	8					
			40	up to 200 <sup>[8]</sup>						
			80	up to 433.3 <sup>[8]</sup>						
			160	up to 866.7 <sup>[8]</sup>						

- A1 A2 IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5,000 m. As of 2009, it is only being licensed in the United States by the FCC.
- B1 B2 Assumes short guard interval (SGI) enabled, otherwise reduce each data rate by 10%.

### 802.11-1997 (802.11 legacy)

The original version of the standard IEEE 802.11 was released in 1997 and clarified in 1999, but is today obsolete. It specified two net bit rates of 1 or 2 megabits per second (Mbit/s), plus forward error correction code. It specified three alternative physical layer technologies: diffuse infrared operating at 1 Mbit/s; frequency-hopping spread spectrum operating at 1 Mbit/s or 2 Mbit/s; and direct-sequence spread spectrum operating at 1 Mbit/s or 2 Mbit/s. The latter two radio technologies used microwave transmission over the Industrial Scientific Medical frequency band

at 2.4 GHz. Some earlier WLAN technologies used lower frequencies, such as the U.S. 900 MHz ISM band. Legacy 802.11 with direct-sequence spread spectrum was rapidly supplanted and popularized by 802.11b.

## 802.11a

The 802.11a standard uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer). It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s<sup>[9]</sup>

Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively unused 5 GHz band gives 802.11a a significant advantage. However, this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g. In theory, 802.11a signals are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength and, as a result, cannot penetrate as far as those of 802.11b. In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5 Mbit/s or even 1 Mbit/s at low signal strengths). 802.11a also suffers from interference,<sup>[10]</sup> but locally there may be fewer signals to interfere with, resulting in less interference and better throughput.

## 802.11b

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include microwave ovens, Bluetooth devices, baby monitors, cordless telephones and some amateur radio equipment.

## 802.11g

In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput.<sup>[11]</sup> 802.11g hardware is fully backward compatible with 802.11b hardware and therefore is encumbered with legacy issues that reduce throughput when compared to 802.11a by ~21%.

The then-proposed 802.11g standard was rapidly adopted by consumers starting in January 2003, well before ratification, due to the desire for higher data rates as well as to reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a and b/g in a single mobile adapter card or access point. Details of making b and g work well together occupied much of the lingering technical process; in an 802.11g network, however, activity of an 802.11b participant will reduce the data rate of the overall 802.11g network.

Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band, for example wireless keyboards.

## 802.11-2007

In 2003, task group TGma was authorized to "roll up" many of the amendments to the 1999 version of the 802.11 standard. REVma or 802.11ma, as it was called, created a single document that merged 8 amendments (802.11a, b, d, e, g, h, i, j) with the base standard. Upon approval on March 8, 2007, 802.11REVma was renamed to the then-current base standard **IEEE 802.11-2007**.<sup>[12]</sup>

## 802.11n

802.11n is an amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output antennas (MIMO). 802.11n operates on both the 2.4 GHz and the lesser used 5 GHz bands. The IEEE has approved the amendment and it was published in October 2009.<sup>[13][12]</sup> Prior to the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.

## 802.11-2012

In 2007, task group TGmb was authorized to "roll up" many of the amendments to the 2007 version of the 802.11 standard. REVmb or 802.11mb, as it was called, created a single document that merged ten amendments (802.11k, r, y, n, w, p, z, v, u, s) with the 2007 base standard. In addition much cleanup was done, including a reordering of many of the clauses. Upon publication on March 29, 2012, the new standard was referred to as **IEEE 802.11-2012**.

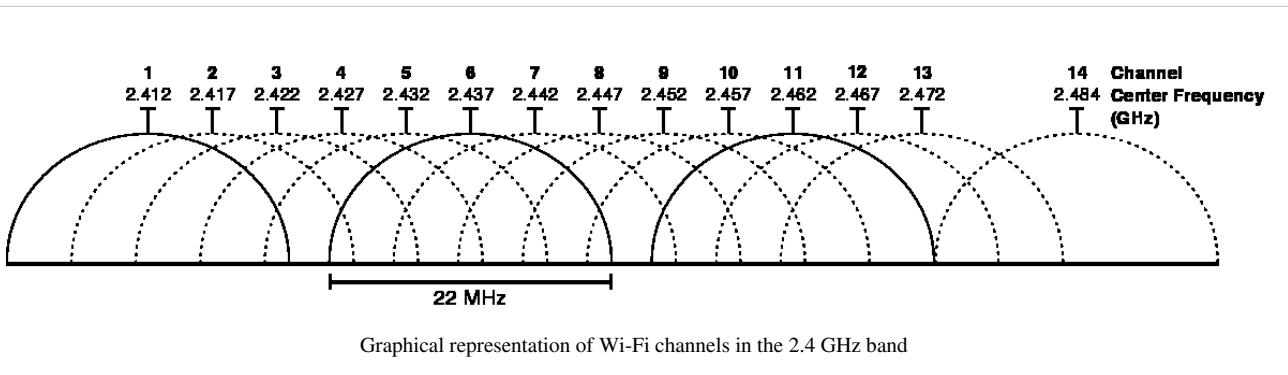
## 802.11ac

IEEE 802.11ac is a standard under development which will provide high throughput in the 5 GHz band. This specification will enable multi-station WLAN throughput of at least 1 gigabits per second and a maximum single link throughput of at least 500 megabits per second, by using wider RF bandwidth (80 or 160 MHz), more streams (up to 8), and high-density modulation (up to 256 QAM).

## 802.11ad

IEEE 802.11ad "WiGig" is a new proposed standard that is already seeing a major push from hardware manufacturers. On 07/24/2012 Marvell and Wilocity announced a new partnership<sup>[14]</sup> to bring a new tri-band Wi-Fi solution to market. Using 2.4GHz, 5GHz and 60GHz, the new standard can achieve a theoretical maximum throughput of up to 7Gbps.<sup>[12]</sup> We can expect to see products beginning to hit the market sometime in early 2014.

## Channels and international compatibility

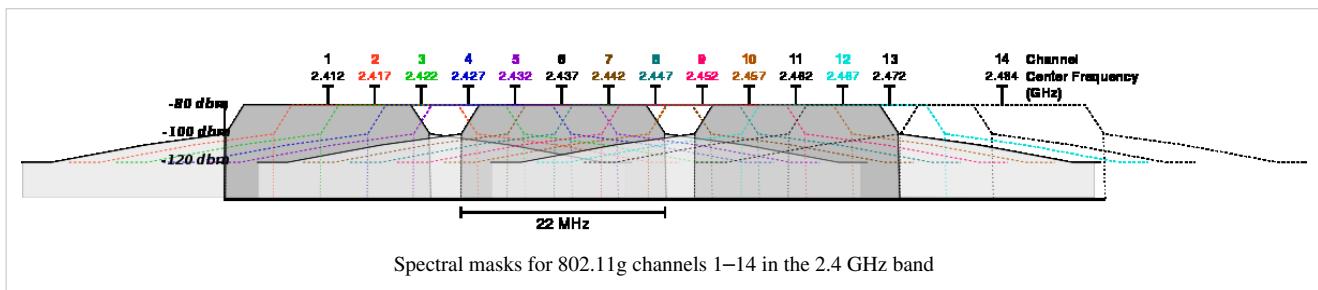
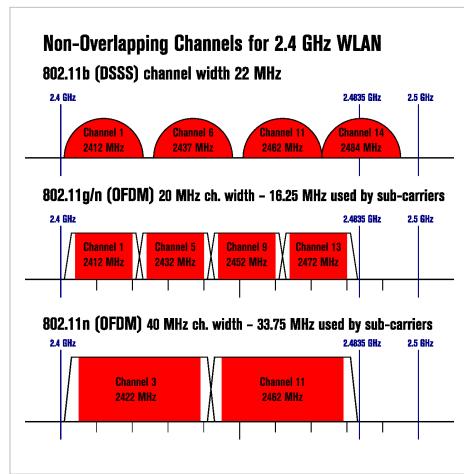


802.11 divides each of the above-described bands into *channels*, analogous to the way radio and TV broadcast bands are sub-divided. For example the 2.4000–2.4835 GHz band is divided into 13 channels spaced 5 MHz apart, with channel 1 centered on 2.412 GHz and 13 on 2.472 GHz (to which Japan added a 14th channel 12 MHz above

channel 13 which was only allowed for 802.11b). 802.11b was based on DSSS with a total channel width of 22 MHz and did not have steep skirts. Consequently only three channels do not overlap. Even now, many devices are shipped with channels 1, 6 and 11 as preset options even though with the newer 802.11g standard there are *four* non-overlapping channels - 1, 5, 9 and 13. There are now four because the OFDM modulated 802.11g channels are 20 MHz wide.

Availability of channels is regulated by country, constrained in part by how each country allocates radio spectrum to various services. At one extreme, Japan permits the use of all 14 channels for 802.11b, while other countries such as Spain initially allowed only channels 10 and 11, and France only allowed 10, 11, 12 and 13. They now allow channels 1 through 13.<sup>[15][16]</sup> North America and some Central and South American countries allow only 1 through 11.

In addition to specifying the channel centre frequency, 802.11 also specifies (in Clause 17) a spectral mask defining the permitted power distribution across each channel. The mask requires the signal be attenuated a minimum of 30 dB from its peak amplitude at  $\pm 11$  MHz from the centre frequency, the point at which a channel is effectively 22 MHz wide. One consequence is that stations can only use every fourth or fifth channel without overlap, typically 1, 6 and 11 in the Americas, and in theory, 1, 5, 9 and 13 in Europe although 1, 6, and 11 is typical there too. Another is that channels 1–13 effectively require the band 2.401–2.483 GHz, the actual allocations being, for example, 2.400–2.4835 GHz in the UK, 2.402–2.4735 GHz in the US, etc.



Since the spectral mask only defines power output restrictions up to  $\pm 11$  MHz from the center frequency to be attenuated by  $-50$  dB<sub>r</sub>, it is often assumed that the energy of the channel extends no further than these limits. It is more correct to say that, given the separation between channels 1, 6, and 11, the signal on any channel should be sufficiently attenuated to minimally interfere with a transmitter on any other channel. Due to the near-far problem a transmitter can impact (desense) a receiver on a "non-overlapping" channel, but only if it is close to the victim receiver (within a meter) or operating above allowed power levels.

Although the statement that channels 1, 6, and 11 are "non-overlapping" is limited to spacing or product density, the 1–6–11 guideline has merit. If transmitters are closer together than channels 1, 6, and 11 (for example, 1, 4, 7, and 10), overlap between the channels may cause unacceptable degradation of signal quality and throughput.<sup>[17]</sup> However, overlapping channels may be used under certain circumstances. This way, more channels are available.<sup>[18]</sup>

A *regdomain* in IEEE 802.11 is a regulatory region. Different countries define different levels of allowable transmitter power, time that a channel can be occupied, and different available channels.<sup>[19]</sup> Domain codes are specified for the United States, Canada, ETSI (Europe), Spain, France, Japan, and China.

Most wifi devices default to regdomain 0, which means least common denominator settings, i.e. the device will not transmit at a power above the allowable power in any nation, nor will it use frequencies that are not permitted in any nation.

The regdomain setting is often made difficult or impossible to change so that the end users do not conflict with local regulatory agencies such as the Federal Communications Commission.

## Frames

Current 802.11 standards define "frame" types for use in transmission of data as well as management and control of wireless links.

Frames are divided into very specific and standardized sections. Each frame consists of a MAC header, payload and frame check sequence (FCS). Some frames may not have the payload. The first two bytes of the MAC header form a frame control field specifying the form and function of the frame. The frame control field is further subdivided into the following sub-fields:

- **Protocol Version:** two bits representing the protocol version. Currently used protocol version is zero. Other values are reserved for future use.
- **Type:** two bits identifying the type of WLAN frame. Control, Data and Management are various frame types defined in IEEE 802.11.
- **Sub Type:** Four bits providing addition discrimination between frames. Type and Sub type together to identify the exact frame.
- **ToDS and FromDS:** Each is one bit in size. They indicate whether a data frame is headed for a distribution system. Control and management frames set these values to zero. All the data frames will have one of these bits set. However communication within an IBSS network always set these bits to zero.
- **More Fragments:** The More Fragments bit is set when a packet is divided into multiple frames for transmission. Every frame except the last frame of a packet will have this bit set.
- **Retry:** Sometimes frames require retransmission, and for this there is a Retry bit which is set to one when a frame is resent. This aids in the elimination of duplicate frames.
- **Power Management:** This bit indicates the power management state of the sender after the completion of a frame exchange. Access points are required to manage the connection and will never set the power saver bit.
- **More Data:** The More Data bit is used to buffer frames received in a distributed system. The access point uses this bit to facilitate stations in power saver mode. It indicates that at least one frame is available and addresses all stations connected.
- **WEP:** The WEP bit is modified after processing a frame. It is toggled to one after a frame has been decrypted or if no encryption is set it will have already been one.
- **Order:** This bit is only set when the "strict ordering" delivery method is employed. Frames and fragments are not always sent in order as it causes a transmission performance penalty.

The next two bytes are reserved for the Duration ID field. This field can take one of three forms: Duration, Contention-Free Period (CFP), and Association ID (AID).

An 802.11 frame can have up to four address fields. Each field can carry a MAC address. Address 1 is the receiver, Address 2 is the transmitter, Address 3 is used for filtering purposes by the receiver.

- The Sequence Control field is a two-byte section used for identifying message order as well as eliminating duplicate frames. The first 4 bits are used for the fragmentation number and the last 12 bits are the sequence number.
- An optional two-byte Quality of Service control field which was added with 802.11e.
- The Frame Body field is variable in size, from 0 to 2304 bytes plus any overhead from security encapsulation and contains information from higher layers.
- The Frame Check Sequence (FCS) is the last four bytes in the standard 802.11 frame. Often referred to as the Cyclic Redundancy Check (CRC), it allows for integrity check of retrieved frames. As frames are about to be sent

the FCS is calculated and appended. When a station receives a frame it can calculate the FCS of the frame and compare it to the one received. If they match, it is assumed that the frame was not distorted during transmission.<sup>[20]</sup>

Management Frames allow for the maintenance of communication. Some common 802.11 subtypes include:

- Authentication frame: 802.11 authentication begins with the WNIC sending an authentication frame to the access point containing its identity. With an open system authentication the WNIC only sends a single authentication frame and the access point responds with an authentication frame of its own indicating acceptance or rejection. With shared key authentication, after the WNIC sends its initial authentication request it will receive an authentication frame from the access point containing challenge text. The WNIC sends an authentication frame containing the encrypted version of the challenge text to the access point. The access point ensures the text was encrypted with the correct key by decrypting it with its own key. The result of this process determines the WNIC's authentication status.
- Association request frame: sent from a station it enables the access point to allocate resources and synchronize. The frame carries information about the WNIC including supported data rates and the SSID of the network the station wishes to associate with. If the request is accepted, the access point reserves memory and establishes an association ID for the WNIC.
- Association response frame: sent from an access point to a station containing the acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such as an association ID and supported data rates.
- Beacon frame: Sent periodically from an access point to announce its presence and provide the SSID, and other parameters for WNICS within range.
- Deauthentication frame: Sent from a station wishing to terminate connection from another station.
- Disassociation frame: Sent from a station wishing to terminate connection. It's an elegant way to allow the access point to relinquish memory allocation and remove the WNIC from the association table.
- Probe request frame: Sent from a station when it requires information from another station.
- Probe response frame: Sent from an access point containing capability information, supported data rates, etc., after receiving a probe request frame.
- Reassociation request frame: A WNIC sends a reassociation request when it drops from range of the currently associated access point and finds another access point with a stronger signal. The new access point coordinates the forwarding of any information that may still be contained in the buffer of the previous access point.
- Reassociation response frame: Sent from an access point containing the acceptance or rejection to a WNIC reassociation request frame. The frame includes information required for association such as the association ID and supported data rates.

Control frames facilitate in the exchange of data frames between stations. Some common 802.11 control frames include:

- Acknowledgement (ACK) frame: After receiving a data frame, the receiving station will send an ACK frame to the sending station if no errors are found. If the sending station doesn't receive an ACK frame within a predetermined period of time, the sending station will resend the frame.
- Request to Send (RTS) frame: The RTS and CTS frames provide an optional collision reduction scheme for access points with hidden stations. A station sends a RTS frame to as the first step in a two-way handshake required before sending data frames.
- Clear to Send (CTS) frame: A station responds to an RTS frame with a CTS frame. It provides clearance for the requesting station to send a data frame. The CTS provides collision control management by including a time value for which all other stations are to hold off transmission while the requesting stations transmits.

Data frames carry packets from web pages, files, etc. within the body<sup>[21]</sup>, using RFC 1042 encapsulation and EtherType numbers for protocol identification.<sup>[22]</sup>

## Standard and amendments

Within the IEEE 802.11 Working Group,<sup>[5]</sup> the following IEEE Standards Association Standard and Amendments exist:

- IEEE 802.11-1997: The WLAN standard was originally 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared (IR) standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.
- IEEE 802.11a: 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b: Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c: Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d: International (country-to-country) roaming extensions (2001)
- IEEE 802.11e: Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F: Inter-Access Point Protocol (2003) Withdrawn February 2006
- IEEE 802.11g: 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h: Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i: Enhanced security (2004)
- IEEE 802.11j: Extensions for Japan (2004)
- IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i and j. (July 2007)
- IEEE 802.11k: Radio resource measurement enhancements (2008)
- IEEE 802.11n: Higher throughput improvements using MIMO (multiple input, multiple output antennas) (September 2009)
- IEEE 802.11p: WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (July 2010)
- IEEE 802.11r: Fast BSS transition (FT) (2008)
- IEEE 802.11s: Mesh Networking, Extended Service Set (ESS) (July 2011)
- IEEE 802.11T: Wireless Performance Prediction (WPP)—test methods and metrics Recommendation cancelled
- IEEE 802.11u: Improvements related to HotSpots and 3rd party authorization of clients, e.g. cellular network offload (February 2011)
- IEEE 802.11v: Wireless network management (February 2011)
- IEEE 802.11w: Protected Management Frames (September 2009)
- IEEE 802.11y: 3650–3700 MHz Operation in the U.S. (2008)
- IEEE 802.11z: Extensions to Direct Link Setup (DLS) (September 2010)
- IEEE 802.11-2012: A new release of the standard that includes amendments k, n, p, r, s, u, v, w, y and z (March 2012)
- IEEE 802.11aa: Robust streaming of Audio Video Transport Streams (June 2012)
- IEEE 802.11ae: Prioritization of Management Frames (March 2012)

## In process

- IEEE 802.11ac: Very High Throughput <6 GHz;<sup>[23]</sup> potential improvements over 802.11n: better modulation scheme (expected ~10% throughput increase), wider channels (estimate in future time 80 to 160 MHz), multi user MIMO;<sup>[24]</sup> (*~ December 2013*)
- IEEE 802.11ad: Very High Throughput 60 GHz (*~ December 2012*) - see WiGig
- IEEE 802.11af: TV Whitespace (*~ June 2014*)
- IEEE 802.11ah: Sub 1 GHz sensor network, smart metering. (*~ May 2015*)
- IEEE 802.11ai: Fast Initial Link Setup (*~ September 2014*)

To reduce confusion, no standard or task group was named 802.11l, 802.11o, 802.11q, 802.11x, 802.11ab, or 802.11ag.

802.11F and 802.11T are recommended practices rather than standards, and are capitalized as such.

802.11m is used for standard maintenance. 802.11ma was completed for 802.11-2007 and 802.11mb was completed for 802.11-2012.

## Standard or amendment?

Both the terms "standard" and "amendment" are used when referring to the different variants of IEEE standards.

As far as the IEEE Standards Association is concerned, there is only one current standard; it is denoted by IEEE 802.11 followed by the date that it was published. IEEE 802.11-2012 is the only version currently in publication. The standard is updated by means of amendments. Amendments are created by task groups (TG). Both the task group and their finished document are denoted by 802.11 followed by a non-capitalized letter. For example IEEE 802.11a and IEEE 802.11b. Updating 802.11 is the responsibility of task group m. In order to create a new version, TGm combines the previous version of the standard and all published amendments. TGm also provides clarification and interpretation to industry on published documents. New versions of the **IEEE 802.11** were published in 1999, 2007 and 2012.

The working title of 802.11-2007 was 802.11-REVma. This denotes a third type of document, a "revision". The complexity of combining 802.11-1999 with 8 amendments made it necessary to revise already agreed upon text. As a result, additional guidelines associated with a revision had to be followed.

## Nomenclature

Various terms in 802.11 are used to specify aspects of wireless local-area networking operation, and may be unfamiliar to some readers.

For example, Time Unit (usually abbreviated TU) is used to indicate a unit of time equal to 1024 microseconds. Numerous time constants are defined in terms of TU (rather than the nearly equal millisecond).

Also the term "Portal" is used to describe an entity that is similar to an 802.1H bridge. A Portal provides access to the WLAN by non-802.11 LAN STAs.

## Community networks

With the proliferation of cable modems and DSL, there is an ever-increasing market of people who wish to establish small networks in their homes to share their broadband Internet connection.

Many hotspot or free networks frequently allow anyone within range, including passersby outside, to connect to the Internet. There are also efforts by volunteer groups to establish wireless community networks to provide free wireless connectivity to the public.

## Security

In 2001, a group from the University of California, Berkeley presented a paper describing weaknesses in the 802.11 Wired Equivalent Privacy (WEP) security mechanism defined in the original standard; they were followed by Fluhrer, Mantin, and Shamir's paper titled "Weaknesses in the Key Scheduling Algorithm of RC4". Not long after, Adam Stubblefield and AT&T publicly announced the first verification of the attack. In the attack, they were able to intercept transmissions and gain unauthorized access to wireless networks.

The IEEE set up a dedicated task group to create a replacement security solution, 802.11i (previously this work was handled as part of a broader 802.11e effort to enhance the MAC layer). The Wi-Fi Alliance announced an interim specification called Wi-Fi Protected Access (WPA) based on a subset of the then current IEEE 802.11i draft. These started to appear in products in mid-2003. IEEE 802.11i (also known as WPA2) itself was ratified in June 2004, and uses government strength encryption in the Advanced Encryption Standard AES, instead of RC4, which was used in

WEP. The modern recommended encryption for the home/consumer space is WPA2 (AES Pre-Shared Key) and for the Enterprise space is WPA2 along with a RADIUS authentication server (or another type of authentication server) and a strong authentication method such as EAP-TLS.

In January 2005, the IEEE set up yet another task group "w" to protect management and broadcast frames, which previously were sent unsecured. Its standard was published in 2009.<sup>[25]</sup>

In December 2011, a security flaw was revealed that affects wireless routers with the optional Wi-Fi Protected Setup (WPS) feature. While WPS is not a part of 802.11, the flaw allows a remote attacker to recover the WPS PIN and, with it, the router's 802.11i password in a few hours.<sup>[26][27]</sup>

## Non-standard 802.11 extensions and equipment

Many companies implement wireless networking equipment with non-IEEE standard 802.11 extensions either by implementing proprietary or draft features. These changes may lead to incompatibilities between these extensions.

## References

- *IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*<sup>[28]</sup>. (2007 revision). IEEE-SA. 12 June 2007. doi:10.1109/IEEESTD.2007.373646.
  - *IEEE 802.11k-2008—Amendment 1: Radio Resource Measurement of Wireless LANs*<sup>[29]</sup>. IEEE-SA. 12 June 2008. doi:10.1109/IEEESTD.2008.4544755.
  - *IEEE 802.11r-2008—Amendment 2: Fast Basic Service Set (BSS) Transition*<sup>[30]</sup>. IEEE-SA. 15 July 2008. doi:10.1109/IEEESTD.2008.4573292.
  - *IEEE 802.11y-2008—Amendment 3: 3650–3700 MHz Operation in USA*<sup>[31]</sup>. IEEE-SA. 6 November 2008. doi:10.1109/IEEESTD.2008.4669928.
- [1] "ARRLWeb: Part 97 - Amateur Radio Service" (<http://www.arrl.org/FandES/field/regulations/news/part97/>). American Radio Relay League. . Retrieved 2010-09-27.
- [2] "Wi-Fi (wireless networking technology)" (<http://www.britannica.com/EBchecked/topic/1473553/Wi-Fi>). Encyclopædia Britannica. . Retrieved 2010-02-03.
- [3] Wolter Lemstra , Vic Hayes , John Groenewegen , *The Innovation Journey of Wi-Fi: The Road To Global Success*, Cambridge University Press, 2010, ISBN 0-521-19971-9
- [4] "Wi-Fi Alliance: Organization" (<http://www.wi-fi.org/organization.php>). Official industry association web site. . Retrieved August 23, 2011.
- [5] "Official IEEE 802.11 working group project timelines" ([http://grouper.ieee.org/groups/802/11/Reports/802.11\\_Timelines.htm](http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm)). Sept. 19, 2009. . Retrieved 2009-10-09.
- [6] "Wi-Fi CERTIFIED n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi® Networks" ([http://www.wi-fi.org/register.php?file=wp\\_Wi-Fi\\_CERTIFIED\\_n\\_Industry.pdf](http://www.wi-fi.org/register.php?file=wp_Wi-Fi_CERTIFIED_n_Industry.pdf)) (registration required). Wi-Fi Alliance. September 2009. .
- [7] "802.11n Delivers Better Range" (<http://www.wi-fiplanet.com/tutorials/article.php/3680781>). Wi-Fi Planet. 2007-05-31. .
- [8] "IEEE802.11ac: The Next Evolution of Wi-Fi Standards" (<http://www.qualcomm.com/media/documents/files/ieee802-11ac-the-next-evolution-of-wi-fi.pdf>). 2012-05-11. . Retrieved 2012-05-16.
- [9] [http://www.oreillynet.com/wireless/2003/08/08/wireless\\_throughput.html](http://www.oreillynet.com/wireless/2003/08/08/wireless_throughput.html)
- [10] Angelakis, V.; Papadakis, S.; Siris, V.A.; Traganitis, A. (March 2011), "Adjacent channel interference in 802.11a is harmful: Testbed validation of a simple quantification model" (<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05723815>), *Communications Magazine (IEEE)* **49** (3): 160–166, doi:10.1109/MCOM.2011.5723815, ISSN 0163-6804,
- [11] *Wireless Networking in the Developing World: A practical guide to planning and building low-cost telecommunications infrastructure* (<http://wndw.net/pdf/wndw2-en/wndw2-ebook.pdf>) (2nd ed.). Hacker Friendly LLC. 2007. p. 425. . page 14
- [12] IEEE 802.11-2007
- [13] "IEEE-SA - News & Events" ([http://standards.ieee.org/announcements/ieee802.11n\\_2009amendment\\_ratified.html](http://standards.ieee.org/announcements/ieee802.11n_2009amendment_ratified.html)). Standards.ieee.org. . Retrieved 2012-05-24.
- [14] "Tri-Band Chip Partnership" (<http://www.brightsideofnews.com/news/2012/7/24/marvell-and-wilocity-partner-up-to-deliver-60ghz-80211ad-wi-fi.aspx>). BRIGHT SIDE OF NEWS. . Retrieved 2012-07-24.
- [15] "Cuadro nacional de Atribución de Frecuencias CNAF" (<http://web.archive.org/web/20080213092618/http://www.mityc.es/Telecomunicaciones/Secciones/Espectro/cnaf>). Secretaría de Estado de Telecomunicaciones. Archived from the original (<http://www.mityc.es/Telecomunicaciones/Secciones/Espectro/cnaf>) on 2008-02-13. . Retrieved 2008-03-05.

- [16] "Evolution du régime d'autorisation pour les RLAN" ([http://www.arcep.fr/uploads/tx\\_gspublication/evol-rlan-250703.pdf](http://www.arcep.fr/uploads/tx_gspublication/evol-rlan-250703.pdf)). French Telecommunications Regulation Authority (ART). . Retrieved 2008-10-26.
- [17] "Channel Deployment Issues for 2.4 GHz 802.11 WLANs" (<http://www.cisco.com/en/US/docs/wireless/technology/channel/deployment/guide/Channel.html>). Cisco Systems, Inc. . Retrieved 2007-02-07.
- [18] Garcia Villegas, E.; et al. (2007). "Effect of adjacent-channel interference in IEEE 802.11 WLANs" ([https://upcommons.upc.edu/e-prints/bitstream/2117/1234/1/CrownCom07\\_CReady.pdf](https://upcommons.upc.edu/e-prints/bitstream/2117/1234/1/CrownCom07_CReady.pdf)). *CrownCom 2007.. ICST & IEEE*. .
- [19] IEEE Standard 802.11-2007 page 531
- [20] "802.11 Technical Section" (<http://wifi.cs.st-andrews.ac.uk/wififrame.html>). . Retrieved 2008-12-15.
- [21] "Understanding 802.11 Frame Types" (<http://www.wi-fiplanet.com/tutorials/article.php/1447501>). . Retrieved 2008-12-14.
- [22] Olivier Bonaventure. "Computer Networking : Principles, Protocols and Practice" (<https://scm.info.ucl.ac.be/release/cnp3/Book/0.2/html/lan/lan.html#wireless-networks>). . Retrieved 2012-07-09.
- [23] "IEEE P802.11 - TASK GROUP AC" ([http://www.ieee802.org/11/Reports/tgac\\_update.htm](http://www.ieee802.org/11/Reports/tgac_update.htm)). IEEE. November 2009. . Retrieved 2009-12-13.
- [24] Fleishman, Glenn (December 7, 2009). "The future of WiFi: gigabit speeds and beyond" (<http://arstechnica.com/business/guides/2009/12/wifi-looks-to-1-gigabit-horizon.ars/1>). Ars Technica. . Retrieved 2009-12-13.
- [25] Jesse Walker, Chair (May 2009). "Status of Project IEEE 802.11 Task Group w: Protected Management Frames" ([http://grouper.ieee.org/groups/802/11/Reports/tgw\\_update.htm](http://grouper.ieee.org/groups/802/11/Reports/tgw_update.htm)). . Retrieved August 23, 2011.
- [26] [http://sviehb.files.wordpress.com/2011/12/viehboeck\\_wps.pdf](http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf)
- [27] <http://www.kb.cert.org/vuls/id/723755> US CERT Vulnerability Note VU#723755
- [28] <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>
- [29] <http://standards.ieee.org/getieee802/download/802.11k-2008.pdf>
- [30] <http://standards.ieee.org/getieee802/download/802.11r-2008.pdf>
- [31] <http://standards.ieee.org/getieee802/download/802.11y-2008.pdf>

## External links

- IEEE 802.11 working group (<http://www.ieee802.org/11/>)
- Purchase the IEEE 802.11-2012 standard from IEEE, published 29 March, 2012 ([http://www.techstreet.com/cgi-bin/detail?vendor\\_id=4523](http://www.techstreet.com/cgi-bin/detail?vendor_id=4523)) (Will return to the free GET IEEE Program (<http://standards.ieee.org/about/get/>) after 6 months of publication)
- Official 802.11 timeline standards from IEEE ([http://www.ieee802.org/11/Reports/802.11\\_Timelines.htm](http://www.ieee802.org/11/Reports/802.11_Timelines.htm))

# IEEE 802.11 (legacy mode)

**IEEE 802.11 (legacy mode)** — or more correctly **IEEE 802.11-1997** or **IEEE 802.11-1999** — refer to the original version of the IEEE 802.11 wireless networking standard released in 1997 and clarified in 1999. Most of the protocols described by this early version are rarely used today.

## Description

It specified two raw data rates of 1 and 2 megabits per second (Mbit/s) to be transmitted via infrared (IR) signals or by either frequency hopping or direct-sequence spread spectrum (DSSS) in the Industrial Scientific Medical frequency band at 2.4 GHz. IR remains a part of the standard but has no actual implementations.

The original standard also defines carrier sense multiple access with collision avoidance (CSMA/CA) as the medium access method. A significant percentage of the available raw channel capacity is sacrificed (via the CSMA/CA mechanisms) in order to improve the reliability of data transmissions under diverse and adverse environmental conditions.

At least six different, somewhat-interoperable, commercial products appeared using the original specification, from companies like Alvarion (PRO.11 and BreezeAccess-II), BreezeCom, Digital / Cabletron (RoamAbout), Lucent, Netwave Technologies (AirSurfer Plus and AirSurfer Pro), Symbol Technologies (Spectrum24), and Proxim Wireless (OpenAir and Rangelan2). A weakness of this original specification was that it offered so many choices that interoperability was sometimes challenging to realize. It is really more of a "beta-specification" than a rigid specification, initially allowing individual product vendors the flexibility to differentiate their products but with little to no inter-vendor operability.

The DSSS version of legacy 802.11 was rapidly supplemented (and popularized) by the 802.11b amendment in 1999, which increased the bit rate to 11 Mbit/s. Widespread adoption of 802.11 networks only occurred after the release of 802.11b which resulted in multiple interoperable products becoming available from multiple vendors. Consequently comparatively few networks were implemented on the 802.11-1997 standard.

802.11 protocol	Release <sup>[1]</sup>	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s) <sup>[2]</sup>	Allowable MIMO streams	Modulation	Approximate indoor range		Approximate outdoor range	
							(m)	(ft)	(m)	(ft)
—	Jun 1997	2.4	20	1, 2	1	DSSS, FHSS	20	unknown operator: u'strong'	100	unknown operator: u'strong'
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	unknown operator: u'strong'	120	unknown operator: u'strong'
		3.7 <sup>[A]</sup>					—	—	5000	unknown operator: u'strong' <sup>[A]</sup>
b	Sep 1999	2.4	20	1, 2, 5.5, 11	1	DSSS	35	unknown operator: u'strong'	140	unknown operator: u'strong'
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	unknown operator: u'strong'	140	unknown operator: u'strong'

n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 <sup>[B]</sup>	4	OFDM	70	<b>unknown operator:</b> <code>u'strong'</code>	250	<b>unknown operator:</b> <code>u'strong'</code> <sup>[3]</sup>
			40	15, 30, 45, 60, 90, 120, 135, 150 <sup>[B]</sup>			70	<b>unknown operator:</b> <code>u'strong'</code>	250	<b>unknown operator:</b> <code>u'strong'</code> <sup>[3]</sup>
ac (DRAFT)	Nov. 2011	5	20	up to 87.6 <sup>[4]</sup>	8					
			40	up to 200 <sup>[4]</sup>						
			80	up to 433.3 <sup>[4]</sup>						
			160	up to 866.7 <sup>[4]</sup>						

- A<sup>1</sup> A<sup>2</sup> IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5,000 m. As of 2009, it is only being licensed in the United States by the FCC.
- B<sup>1</sup> B<sup>2</sup> Assumes short guard interval (SGI) enabled, otherwise reduce each data rate by 10%.

## References

- [1] "Official IEEE 802.11 working group project timelines" ([http://grouper.ieee.org/groups/802/11/Reports/802.11\\_Timelines.htm](http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm)). Sept. 19, 2009. . Retrieved 2009-10-09.
- [2] "Wi-Fi CERTIFIED n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi® Networks" ([http://www.wi-fi.org/register.php?file=wp\\_Wi-Fi\\_CERTIFIED\\_n\\_Industry.pdf](http://www.wi-fi.org/register.php?file=wp_Wi-Fi_CERTIFIED_n_Industry.pdf)) (registration required). *Wi-Fi Alliance*. September 2009. .
- [3] "802.11n Delivers Better Range" (<http://www.wi-fiplanet.com/tutorials/article.php/3680781>). *Wi-Fi Planet*. 2007-05-31. .
- [4] "IEEE802.11ac: The Next Evolution of Wi-Fi Standards" (<http://www.qualcomm.com/media/documents/files/ieee802-11ac-the-next-evolution-of-wi-fi.pdf>). 2012-05-11. . Retrieved 2012-05-16.

## Further reading

- IEEE 802.11 Working Group (1997-11-18). *IEEE 802.11-1997: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* ([http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?isnumber=14251&arnumber=654749&count=1&index=0](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?isnumber=14251&arnumber=654749&count=1&index=0)). ISBN 1-55937-935-9.
- IEEE 802.11 Working Group (1999-07-15). *IEEE 802.11-1999: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* ([http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?tp=&isnumber=30234&arnumber=1389197&punumber=9543](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&isnumber=30234&arnumber=1389197&punumber=9543)). ISBN 0-7381-1857-5.

# IEEE 802.11a-1999

**IEEE 802.11a-1999** or **802.11a** is an amendment to the IEEE 802.11 specification that added a higher data rate of up to 54 Mbit/s using the 5 GHz band. It has seen widespread worldwide implementation, particularly within the corporate workspace. The amendment has been incorporated into the published IEEE 802.11-2007 standard.

802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in their 802.11a, 802.11b, 802.11g and 802.11n versions to provide wireless connectivity in the home, office and some commercial establishments.

## Description

The 802.11a amendment to the original standard was ratified in 1999. The 802.11a standard uses the same core protocol as the original standard, operates in 5 GHz band, and uses a 52-subcarrier orthogonal frequency-division multiplexing (OFDM) with a maximum raw data rate of 54 Mbit/s, which yields realistic net achievable throughput in the mid-20 Mbit/s. The data rate is reduced to 48, 36, 24, 18, 12, 9 then 6 Mbit/s if required. 802.11a originally had 12/13 non-overlapping channels, 12 that can be used indoor and 4/5 of the 12 that can be used in outdoor point to point configurations. Recently many countries of the world are allowing operation in the 5.47 to 5.725 GHz Band as a secondary user using a sharing method derived in 802.11h. This will add another 12/13 Channels to the overall 5 GHz band enabling significant overall wireless network capacity enabling the possibility of 24+ channels in some countries. 802.11a is not interoperable with 802.11b as they operate on separate bands, except if using equipment that has a dual band capability. Most enterprise class Access Points have dual band capability.

Using the 5 GHz band gives 802.11a a significant advantage, since the 2.4 GHz band is heavily used to the point of being crowded. Degradation caused by such conflicts can cause frequent dropped connections and degradation of service. However, this high carrier frequency also brings a slight disadvantage: The effective overall range of 802.11a is slightly less than that of 802.11b/g; 802.11a signals cannot penetrate as far as those for 802.11b because they are absorbed more readily by walls and other solid objects in their path and because the path loss in signal strength is proportional to the square of the signal frequency. On the other hand, OFDM has fundamental propagation advantages when in a high multipath environment, such as an indoor office, and the higher frequencies enable the building of smaller antennas with higher RF system gain which counteract the disadvantage of a higher band of operation. The increased number of usable channels (4 to 8 times as many in FCC countries) and the near absence of other interfering systems (microwave ovens, cordless phones, baby monitors) give 802.11a significant aggregate bandwidth and reliability advantages over 802.11b/g.

## Regulatory issues

Different countries have different regulatory support, although a 2003 World Radiotelecommunications Conference improved worldwide standards coordination. 802.11a is now approved by regulations in the United States and Japan, but in other areas, such as the European Union, it had to wait longer for approval. European regulators were considering the use of the European HIPERLAN standard, but in mid-2002 cleared 802.11a for use in Europe. In the U.S., a mid-2003 FCC decision may open more spectrum to 802.11a channels.

## Timing and compatibility of products

802.11a products started shipping late, lagging 802.11b products due to 5 GHz components being more difficult to manufacture. First generation product performance was poor and plagued with problems. When second generation products started shipping, 802.11a was not widely adopted in the consumer space primarily because the less-expensive 802.11b was already widely adopted. However, 802.11a later saw significant penetration into enterprise network environments, despite the initial cost disadvantages, particularly for businesses which required increased capacity and reliability over 802.11b/g-only networks.

With the arrival of less expensive early 802.11g products on the market, which were backwards-compatible with 802.11b, the bandwidth advantage of the 5 GHz 802.11a in the consumer market was reduced. Manufacturers of 802.11a equipment responded to the lack of market success by significantly improving the implementations (current-generation 802.11a technology has range characteristics nearly identical to those of 802.11b), and by making technology that can use more than one band a standard.

Dual-band, or dual-mode Access Points and Network Interface Cards (NICs) that can automatically handle a and b/g, are now common in all the markets, and very close in price to b/g- only devices.

## Technical description

Of the 52 OFDM subcarriers, 48 are for data and 4 are pilot subcarriers with a carrier separation of 0.3125 MHz (20 MHz/64). Each of these subcarriers can be a BPSK, QPSK, 16-QAM or 64-QAM. The total bandwidth is 20 MHz with an occupied bandwidth of 16.6 MHz. Symbol duration is 4 microseconds, which *includes* a guard interval of 0.8 microseconds. The actual generation and decoding of orthogonal components is done in baseband using DSP which is then upconverted to 5 GHz at the transmitter. Each of the subcarriers could be represented as a complex number. The time domain signal is generated by taking an Inverse Fast Fourier transform (IFFT). Correspondingly the receiver downconverts, samples at 20 MHz and does an FFT to retrieve the original coefficients. The advantages of using OFDM include reduced multipath effects in reception and increased spectral efficiency.

Mod.	Net (Mbit/s)	Gross (Mbit/s)	FEC rate	Efficiency (bit/sym.)	$T_{1472\text{ B}}$ (μs)
BPSK	6	12	1/2	24	2012
BPSK	9	12	3/4	36	1344
QPSK	12	24	1/2	48	1008
QPSK	18	24	3/4	72	672
16-QAM	24	48	1/2	96	504
16-QAM	36	48	3/4	144	336
64-QAM	48	72	2/3	192	252
64-QAM	54	72	3/4	216	224

## References

- "802.11a-1999 High-speed Physical Layer in the 5 GHz band" [1] (PDF). 1999-02-11. Retrieved 2007-09-24.  
[1] <http://standards.ieee.org/getieee802/download/802.11a-1999.pdf>

# IEEE 802.11b-1999

**IEEE 802.11b-1999** or **802.11b**, is an amendment to the IEEE 802.11 specification that extended throughput up to 11 Mbit/s using the same 2.4 GHz band. This specification under the marketing name of Wi-Fi has been implemented all over the world. The amendment has been incorporated into the published IEEE 802.11-2007 standard.

802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in their 802.11a, 802.11b, 802.11g and 802.11n versions to provide wireless connectivity in the home, office and some commercial establishments.

## Description

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same CSMA/CA media access method defined in the original standard. Due to the CSMA/CA protocol overhead, in practice the maximum 802.11b throughput that an application can achieve is about 5.9 Mbit/s using TCP and 7.1 Mbit/s using UDP.

802.11b products appeared on the market in mid-1999, since 802.11b is a direct extension of the DSSS (Direct-sequence spread spectrum) modulation technique defined in the original standard. The Apple iBook was the first mainstream computer sold with optional 802.11b networking. Technically, the 802.11b standard uses Complementary code keying (CCK) as its modulation technique. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

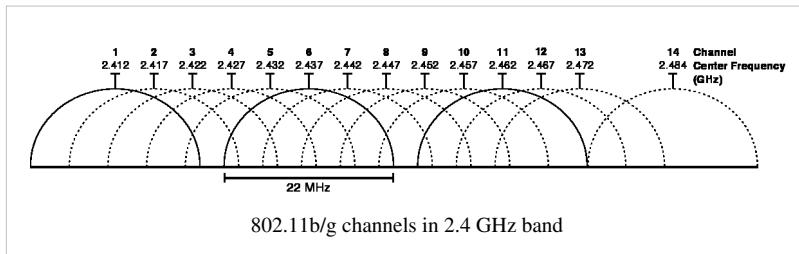
802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and cordless telephones. Interference issues and user density problems within the 2.4 GHz band have become a major concern and frustration for users.

## Range

802.11b is used in a point-to-multipoint configuration, wherein an access point communicates via an omnidirectional antenna with one or more nomadic or mobile clients that are located in a coverage area around the access point. Typical indoor range is 30 m (100 ft) at 11 Mbit/s and 90 m (300 ft) at 1 Mbit/s. The overall bandwidth is dynamically demand shared across all the users on a channel. With high-gain external antennas, the protocol can also be used in fixed point-to-point arrangements, typically at ranges up to 8 kilometers (**unknown operator: u'strong'** mi) although some report success at ranges up to 80–120 km (50–75 miles) where line of sight can be established. This is usually done in place of costly leased lines or very cumbersome microwave communications equipment. Designers of such installations who wish to remain within the law must however be careful about legal limitations on effective radiated power.<sup>[1]</sup>

802.11b cards can operate at 11 Mbit/s, but will scale back to 5.5, then 2, then 1 Mbit/s (also known as Adaptive Rate Selection), if signal quality becomes an issue.

## Channels and Frequencies



**802.11b channel to frequency map** [2]

Channel	Center Frequency	Frequency delta	Channel Width	Overlaps Channels
1	2.412 GHz	5 MHz	2.401–2.423 GHz	2-5
2	2.417 GHz	5 MHz	2.406–2.428 GHz	1,3-6
3	2.422 GHz	5 MHz	2.411–2.433 GHz	1-2,4-7
4	2.427 GHz	5 MHz	2.416–2.438 GHz	1-3,5-8
5	2.432 GHz	5 MHz	2.421–2.443 GHz	1-4,6-9
6	2.437 GHz	5 MHz	2.426–2.448 GHz	2-5,7-10
7	2.442 GHz	5 MHz	2.431–2.453 GHz	3-6,8-11
8	2.447 GHz	5 MHz	2.436–2.458 GHz	4-7,9-12
9	2.452 GHz	5 MHz	2.441–2.463 GHz	5-8,10-13
10	2.457 GHz	5 MHz	2.446–2.468 GHz	6-9,11-13
11	2.462 GHz	5 MHz	2.451–2.473 GHz	7-10,12-13
12	2.467 GHz	5 MHz	2.456–2.478 GHz	8-11,13-14
13	2.472 GHz	5 MHz	2.461–2.483 GHz	9-12, 14
14	2.484 GHz	12 MHz	2.473–2.495 GHz	12-13

*Note: Channel 14 is only allowed in Japan, Channels 12 & 13 are allowed in most parts of the world, except the USA, where only Channels 1 to 11 are legal to use. More information can be found in the List of WLAN channels.*

## References

- [1] "Code of Federal Regulations, Title 47-Telecommunications, Chapter I-Federal Communications Commission, Part 15-Radio Frequency Devices, Section 15.247" ([http://a257.g.akamaitech.net/7/257/2422/13nov20061500/edocket.access.gpo.gov/cfr\\_2006/octqtr/pdf/47cfr15.247.pdf](http://a257.g.akamaitech.net/7/257/2422/13nov20061500/edocket.access.gpo.gov/cfr_2006/octqtr/pdf/47cfr15.247.pdf)). 2006-10-01. . Retrieved 2008-01-09.
- [2] <http://download.wcvirtual.com/reference/802%20Channel%20Freq%20Mappings.pdf>
  - "802.11b-1999 Higher Speed Physical Layer Extension in the 2.4 GHz band" (<http://standards.ieee.org/getieee802/download/802.11b-1999.pdf>) (pdf). 1999-02-11. Retrieved 2007-09-24.
  - "Corrigenda to 802.11b-1999 Higher Speed Physical Layer Extension in the 2.4 GHz band" ([http://standards.ieee.org/getieee802/download/802.11b-1999\\_Cor1-2001.pdf](http://standards.ieee.org/getieee802/download/802.11b-1999_Cor1-2001.pdf)) (pdf). 2002-01-30. Retrieved 2007-09-24.

# IEEE 802.11g-2003

**IEEE 802.11g-2003** or **802.11g** is an amendment to the IEEE 802.11 specification that extended throughput to up to 54 Mbit/s using the same 2.4 GHz band as 802.11b. This specification under the marketing name of Wi-Fi has been implemented all over the world. The 802.11g protocol is now Clause 19 of the published IEEE 802.11-2007 standard.

802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in their 802.11a, 802.11b, 802.11g and 802.11n versions to provide wireless connectivity in the home, office and some commercial establishments.

## Descriptions

802.11g is the third modulation standard for wireless LANs. It works in the 2.4 GHz band (like 802.11b) but operates at a maximum raw data rate of 54 Mbit/s, or about 19 Mbit/s net throughput (identical to 802.11a core, except for some additional legacy overhead for backward compatibility). 802.11g hardware is fully backwards compatible with 802.11b hardware. Details of making b and g work well together occupied much of the lingering technical process. In an 802.11g network, however, the presence of a legacy 802.11b participant will significantly reduce the speed of the overall 802.11g network.

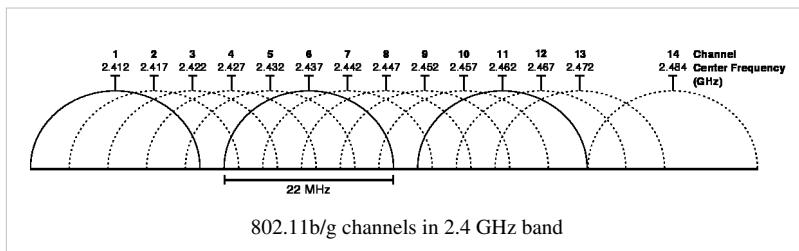
The modulation scheme used in 802.11g is orthogonal frequency-division multiplexing (OFDM) copied from 802.11a with data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s, and reverts to CCK (like the 802.11b standard) for 5.5 and 11 Mbit/s and DBPSK/DQPSK+DSSS for 1 and 2 Mbit/s. Even though 802.11g operates in the same frequency band as 802.11b, it can achieve higher data rates because of its heritage to 802.11a.

## Adoption

The then-proposed 802.11g standard was rapidly adopted by consumers starting in January 2003, well before ratification, due to the desire for higher speeds and reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a and b/g in a single mobile adapter card or access point.

Despite its major acceptance, 802.11g suffers from the same interference as 802.11b in the already crowded 2.4 GHz range. Devices operating in this range include microwave ovens, Bluetooth devices, baby monitors and digital cordless telephones, which can lead to interference issues. Additionally, the success of the standard has caused usage/density problems related to crowding in urban areas. To prevent interference, there are only three non-overlapping usable channels in the U.S. and other countries with similar regulations (channels 1, 6, 11, with 25 MHz separation), and four in Europe (channels 1, 5, 9, 13, with only 20 MHz separation). Even with such separation, some interference due to side lobes exists, though it is considerably weaker.

## Channels and Frequencies



### IEEE 802.11g channel to frequency map <sup>[1]</sup>

Channel	Center Frequency	Channel Width	Overlaps Channels
1	2.412 GHz	2.401 GHz - 2.423 GHz	2,3,4,5
2	2.417 GHz	2.406 GHz - 2.428 GHz	1,3,4,5,6
3	2.422 GHz	2.411 GHz - 2.433 GHz	1,2,4,5,6,7
4	2.427 GHz	2.416 GHz - 2.438 GHz	1,2,3,5,6,7,8
5	2.432 GHz	2.421 GHz - 2.443 GHz	1,2,3,4,6,7,8,9
6	2.437 GHz	2.426 GHz - 2.448 GHz	2,3,4,5,7,8,9,10
7	2.442 GHz	2.431 GHz - 2.453 GHz	3,4,5,6,8,9,10,11
8	2.447 GHz	2.436 GHz - 2.458 GHz	4,5,6,7,9,10,11,12
9	2.452 GHz	2.441 GHz - 2.463 GHz	5,6,7,8,10,11,12,13
10	2.457 GHz	2.446 GHz - 2.468 GHz	6,7,8,9,11,12,13
11	2.462 GHz	2.451 GHz - 2.473 GHz	7,8,9,10,12,13
12	2.467 GHz	2.456 GHz - 2.478 GHz	8,9,10,11,13
13	2.472 GHz	2.461 GHz - 2.483 GHz	9,10,11,12
14	2.484 GHz	2.473 GHz - 2.495 GHz	12,13

*Note: Not all channels are legal to use in all countries.*

## References

- "IEEE 802.11g-2003: Further Higher Data Rate Extension in the 2.4 GHz Band" <sup>[2]</sup> (pdf). IEEE. 2003-10-20.  
Retrieved 2007-09-24.

[1] <http://download.wcvirtual.com/reference/802%20Channel%20Freq%20Mappings.pdf>

[2] <http://standards.ieee.org/getieee802/download/802.11g-2003.pdf>

# IEEE 802.11n-2009

**IEEE 802.11n-2009** is an amendment to the IEEE 802.11-2007 wireless networking standard to improve network throughput over the two previous standards—802.11a and 802.11g—with a significant increase in the maximum net data rate from 54 Mbit/s to 600 Mbit/s (slightly higher gross bit rate including for example error-correction codes, and slightly lower maximum throughput) with the use of four spatial streams at a channel width of 40 MHz.<sup>[1][2]</sup> 802.11n standardized support for multiple-input multiple-output and frame aggregation, and security improvements, among other features.

802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in their 802.11a, 802.11b, 802.11g, and 802.11n versions to provide wireless connectivity in homes and businesses. Development of 802.11n began in 2002, seven years before publication. Proposed enhancements to 802.11n are under development as part of IEEE 802.11ac.

## Description

IEEE 802.11n is an amendment to IEEE 802.11-2007 as amended by IEEE 802.11k-2008, IEEE 802.11r-2008, IEEE 802.11y-2008, and IEEE 802.11w-2009, and builds on previous 802.11 standards by adding multiple-input multiple-output (MIMO) and 40 MHz channels to the PHY (physical layer), and frame aggregation to the MAC layer.

MIMO is a technology that uses multiple antennas to coherently resolve more information than possible using a single antenna. One way it provides this is through Spatial Division Multiplexing (SDM), which spatially multiplexes multiple independent data streams, transferred simultaneously within one spectral channel of bandwidth. MIMO SDM can significantly increase data throughput as the number of resolved spatial data streams is increased. Each spatial stream requires a discrete antenna at both the transmitter and the receiver. In addition, MIMO technology requires a separate radio-frequency chain and analog-to-digital converter for each MIMO antenna, making it more expensive to implement than non-MIMO systems.

Channels operating with a width of 40 MHz are another feature incorporated into 802.11n; this doubles the channel width from 20 MHz in previous 802.11 PHYs to transmit data, and provides twice the PHY data rate available over a single 20 MHz channel. It can be enabled in the 5 GHz mode, or within the 2.4 GHz if there is knowledge that it will not interfere with any other 802.11 or non-802.11 (such as Bluetooth) system using the same frequencies.<sup>[3]</sup>

MIMO architecture, together with wider-bandwidth channels, offers increased physical transfer rate over 802.11a (5 GHz) and 802.11g (2.4 GHz).<sup>[4]</sup>

## Data encoding

The transmitter and receiver use precoding and postcoding techniques, respectively, to achieve the capacity of a MIMO link. Precoding includes spatial beamforming and spatial coding, where spatial beamforming improves the received signal quality at the decoding stage. Spatial coding can increase data throughput via spatial multiplexing and increase range by exploiting the spatial diversity, through techniques such as Alamouti coding.

## Number of antennas

The number of simultaneous data streams is limited by the minimum number of antennas in use on both sides of the link. However, the individual radios often further limit the number of spatial streams that may carry unique data. The  $a \times b : c$  notation helps identify what a given radio is capable of. The first number (a) is the maximum number of transmit antennas or RF chains that can be used by the radio. The second number (b) is the maximum number of receive antennas or RF chains that can be used by the radio. The third number (c) is the maximum number of data spatial streams the radio can use. For example, a radio that can transmit on two antennas and receive on three, but

can only send or receive two data streams would be  $2 \times 3 : 2$ .

The 802.11n draft allows up to  $4 \times 4 : 4$ . Common configurations of 11n devices are  $2 \times 2 : 2$ ;  $2 \times 3 : 2$ ; and  $3 \times 2 : 2$ . All three configurations have the same maximum throughputs and features, and differ only in the amount of diversity the antenna systems provide. In addition, a fourth configuration,  $3 \times 3 : 3$  is becoming common, which has a higher throughput, due to the additional data stream.<sup>[5]</sup>

## Data rates

Data rates up to 600 Mbit/s are achieved only with the maximum of four spatial streams using one 40 MHz-wide channel. Various modulation schemes and coding rates are defined by the standard and are represented by a Modulation and Coding Scheme (MCS) index value. The table below shows the relationships between the variables that allow for the maximum data rate.<sup>[6]</sup>

MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
<b>0</b>	1	BPSK	1/2	6.50	7.20	13.50	15.00
<b>1</b>	1	QPSK	1/2	13.00	14.40	27.00	30.00
<b>2</b>	1	QPSK	3/4	19.50	21.70	40.50	45.00
<b>3</b>	1	16-QAM	1/2	26.00	28.90	54.00	60.00
<b>4</b>	1	16-QAM	3/4	39.00	43.30	81.00	90.00
<b>5</b>	1	64-QAM	2/3	52.00	57.80	108.00	120.00
<b>6</b>	1	64-QAM	3/4	58.50	65.00	121.50	135.00
<b>7</b>	1	64-QAM	5/6	65.00	72.20	135.00	150.00
<b>8</b>	2	BPSK	1/2	13.00	14.40	27.00	30.00
<b>9</b>	2	QPSK	1/2	26.00	28.90	54.00	60.00
<b>10</b>	2	QPSK	3/4	39.00	43.30	81.00	90.00
<b>11</b>	2	16-QAM	1/2	52.00	57.80	108.00	120.00
<b>12</b>	2	16-QAM	3/4	78.00	86.70	162.00	180.00
<b>13</b>	2	64-QAM	2/3	104.00	115.60	216.00	240.00
<b>14</b>	2	64-QAM	3/4	117.00	130.00	243.00	270.00
<b>15</b>	2	64-QAM	5/6	130.00	144.40	270.00	300.00
<b>16</b>	3	BPSK	1/2	19.50	21.70	40.50	45.00
<b>17</b>	3	QPSK	1/2	39.00	43.30	81.00	90.00
<b>18</b>	3	QPSK	3/4	58.50	65.00	121.50	135.00
<b>19</b>	3	16-QAM	1/2	78.00	86.70	162.00	180.00
<b>20</b>	3	16-QAM	3/4	117.00	130.00	243.00	270.00
<b>21</b>	3	64-QAM	2/3	156.00	173.30	324.00	360.00
<b>22</b>	3	64-QAM	3/4	175.50	195.00	364.50	405.00
<b>23</b>	3	64-QAM	5/6	195.00	216.70	405.00	450.00
<b>24</b>	4	BPSK	1/2	26.00	28.80	54.00	60.00
<b>25</b>	4	QPSK	1/2	52.00	57.60	108.00	120.00

<b>26</b>	4	QPSK	3/4	78.00	86.80	162.00	180.00
<b>27</b>	4	16-QAM	1/2	104.00	115.60	216.00	240.00
<b>28</b>	4	16-QAM	3/4	156.00	173.20	324.00	360.00
<b>29</b>	4	64-QAM	2/3	208.00	231.20	432.00	480.00
<b>30</b>	4	64-QAM	3/4	234.00	260.00	486.00	540.00
<b>31</b>	4	64-QAM	5/6	260.00	288.80	540.00	600.00

## Frame aggregation

PHY level data rate improvements do not increase user level throughput beyond a point because of 802.11 protocol overheads, like the contention process, interframe spacing, PHY level headers (Preamble + PLCP) and acknowledgment frames. The main medium access control (MAC) feature that provides a performance improvement is aggregation. Two types of aggregation are defined:

1. Aggregation of MAC service data units (MSDUs) at the top of the MAC (referred to as MSDU aggregation or A-MSDU)
2. Aggregation of MAC protocol data units (MPDUs) at the bottom of the MAC (referred to as MPDU aggregation or A-MPDU)

Frame aggregation is a process of packing multiple MSDUs or MPDUs together to reduce the overheads and average them over multiple frames, thereby increasing the user level data rate. A-MPDU aggregation requires the use of block acknowledgement or BlockAck, which was introduced in 802.11e and has been optimized in 802.11n.

## Backward compatibility

When 802.11g was released to share the band with existing 802.11b devices, it provided ways of ensuring coexistence between legacy and successor devices. 802.11n extends the coexistence management to protect its transmissions from legacy devices, which include 802.11g, 802.11b and 802.11a. There are MAC and PHY level protection mechanisms as listed below:

1. PHY level protection: Mixed Mode Format protection (also known as L-SIG TXOP Protection): In mixed mode, each 802.11n transmission is always embedded in an 802.11a or 802.11g transmission. For 20 MHz transmissions, this embedding takes care of the protection with 802.11a and 802.11g. However, 802.11b devices still need CTS protection.
2. PHY level protection: Transmissions using a 40 MHz channel in the presence of 802.11a or 802.11g clients require using CTS protection on both 20 MHz halves of the 40 MHz channel, to prevent interference with legacy devices.
3. MAC level protection: An RTS/CTS frame exchange or CTS frame transmission at legacy rates can be used to protect subsequent 11n transmission.

Even with protection, large discrepancies can exist between the throughput an 802.11n device can achieve in a greenfield network, compared to a mixed-mode network, when legacy devices are present. This is an extension of the 802.11b/802.11g coexistence problem.

## Deployment strategies

To achieve maximum output, a pure 802.11n 5 GHz network is recommended. The 5 GHz band has substantial capacity due to many non-overlapping radio channels and less radio interference as compared to the 2.4 GHz band.<sup>[7]</sup> An 802.11n-only network may be impractical for many users because they need to support legacy equipment that still is 802.11b/g only. Consequently, it may be more practical in the short term to operate a mixed 802.11b/g/n network until 802.11n hardware becomes more prevalent. In a mixed-mode system, an optimal solution would be to

use a dual-radio access point and place the 802.11b/g traffic on the 2.4 GHz radio and the 802.11n traffic on the 5 GHz radio.<sup>[8]</sup> This setup assumes that all the 802.11n clients are 5 GHz capable, which isn't a requirement of the standard. A technique called "band steering" is used by some enterprise-grade APs to send 802.11n clients to the 5 GHz band, leaving the 2.4 GHz band for legacy clients. Band steering works by responding only to 5 GHz association requests and not the 2.4 GHz requests from dual-band clients.<sup>[9]</sup>

## 40 MHz in 2.4 GHz

The 2.4 GHz ISM band is fairly congested. With 802.11n, there is the option to double the bandwidth per channel to 40 MHz which results in slightly more than double the data rate. However, when in 2.4 GHz, enabling this option takes up to 82%<sup>[10]</sup> of the unlicensed band, which in many areas may prove to be infeasible.

The specification calls for requiring one primary 20 MHz channel as well as a secondary adjacent channel spaced  $\pm 20$  MHz away. The primary channel is used for communications with clients incapable of 40 MHz mode. When in 40 MHz mode, the center frequency is actually the mean of the primary and secondary channels.

Primary channel	20 MHz		40 MHz above			40 MHz below		
	Blocks	2nd ch.	Center	Blocks	2nd ch.	Center	Blocks	
1	1-3	5	3	1-7	Not Available			
2	1-4	6	4	1-8	Not Available			
3	1-5	7	5	1-9	Not Available			
4	2-6	8	6	2-10	Not Available			
5	3-7	9	7	3-11	1	3	1-7	
6	4-8	10	8	4-12	2	4	1-8	
7	5-9	11	9	5-13	3	5	1-9	
8	6-10	12	10	6-13	4	6	2-10	
9	7-11	13	11	7-13	5	7	3-11	
10	8-12	Not Available			6	8	4-12	
11	9-13	Not Available			7	9	5-13	
12	10-13	Not Available			8	10	6-13	
13	11-13	Not Available			9	11	7-13	

Local regulations may restrict certain channels from operation. For example, Channels 12 and 13 are normally unavailable for use as either a primary or secondary channel in North America. For further information, see List of WLAN channels.

## Wi-Fi Alliance

As of mid-2007, the Wi-Fi Alliance started certifying products based on IEEE 802.11n draft 2.0.<sup>[11][12]</sup> This certification program established a set of features and a level of interoperability across vendors supporting those features, thus providing one definition of 'draft n'. The baseline certification covers both 20 MHz and 40 MHz wide channels, and up to two spatial streams, for maximum throughputs of 144.4 Mbit/s for 20 MHz and 300 Mbit/s for 40 MHz (with short guard interval). A number of vendors in both the consumer and enterprise spaces have built products that have achieved this certification.<sup>[13]</sup> The Wi-Fi Alliance certification program subsumed the previous industry consortium efforts to define 802.11n, such as the now dormant Enhanced Wireless Consortium (EWC). The Alliance has upgraded its suite of compatibility tests for some enhancements that were finalized after draft 2.0. Furthermore, it has affirmed that all draft-n certified products remain compatible with the products conforming to the

final standards.<sup>[14]</sup> The Wi-Fi Alliance is investigating further work on certification of additional features of 802.11n not covered by the baseline certification, including higher numbers of spatial streams (3 or 4), Greenfield Format, PSMP, implicit and explicit beamforming and space-time block coding.

## Timeline

The following are milestones in the development of 802.11n:<sup>[15]</sup>

September 11, 2002

The first meeting of the High-Throughput Study Group (HTSG) was held. Earlier in the year, in the Wireless Next Generation standing committee (WNG SC), presentations were heard on why they need change and what the target throughput would be required to justify the amendments. Compromise was reached in May 2002 to delay the start of the Study Group until September to allow 11g to complete major work during the July 2002 session.

September 11, 2003

The IEEE-SA New Standards Committee (NesCom) approved the Project Authorization Request (PAR) for the purpose of amending the 802.11-2007 standard. The new 802.11 Task Group (TGn) is to develop a new amendment. The TGn amendment is based on IEEE Std 802.11-2007, as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008 and IEEE P802.11w. TGn will be the 5th amendment to the 802.11-2007 standard. The scope of this project is to define an amendment that shall define standardized modifications to both the 802.11 physical layers (PHY) and the 802.11 Medium Access Control Layer (MAC) so that modes of operation can be enabled that are capable of much higher throughputs, with a maximum throughput of at least 100 Mbit/s, as measured at the MAC data service access point (SAP).

September 15, 2003

The first meeting of the new 802.11 Task Group (TGn).

May 17, 2004

Call for Proposals was issued.

September 13, 2004

32 first round of proposals were heard.

March 2005

Proposals were downselected to a single proposal, but there is not a 75% consensus on the one proposal. Further efforts were expended over the next 3 sessions without being able to agree on one proposal.

July 2005

Previous competitors TGn Sync, WWiSE, and a third group, MITMOT, said that they would merge their respective proposals as a draft. The standardization process was expected to be completed by the second quarter of 2009.

January 19, 2006

The IEEE 802.11n Task Group approved the Joint Proposal's specification, enhanced by EWC's draft specification.

March 2006

IEEE 802.11 Working Group sent the 802.11n draft to its first letter ballot, allowing the 500+ 802.11 voters to review the document and suggest bug fixes, changes, and improvements.

May 2, 2006

The IEEE 802.11 Working Group voted not to forward draft 1.0 of the proposed 802.11n standard. Only 46.6% voted to approve the ballot. To proceed to the next step in the IEEE standards process, a majority vote

of 75% is required. This letter ballot also generated approximately 12,000 comments—many more than anticipated.

November 2006

TGn voted to accept draft version 1.06, incorporating all accepted technical and editorial comment resolutions prior to this meeting. An additional 800 comment resolutions were approved during the November session which will be incorporated into the next revision of the draft. As of this meeting, three of the 18 comment topic ad hoc groups chartered in May had completed their work, and 88% of the technical comments had been resolved, with approximately 370 remaining.

January 19, 2007

The IEEE 802.11 Working Group unanimously (100 yes, 0 no, 5 abstaining) approved a request by the 802.11n Task Group to issue a new draft 2.0 of the proposed standard. Draft 2.0 was based on the Task Group's working draft version 1.10. Draft 2.0 was at this point in time the cumulative result of thousands of changes to the 11n document as based on all previous comments.

February 7, 2007

The results of Letter Ballot 95, a 15-day Procedural vote, passed with 97.99% approval and 2.01% disapproval. On the same day, 802.11 Working Group announced the opening of Letter Ballot 97. It invited detailed technical comments to closed on 9 March 2007.

March 9, 2007

Letter Ballot 97, the 30-day Technical vote to approve draft 2.0, closed. They were announced by IEEE 802 leadership during the Orlando Plenary on 12 March 2007. The ballot passed with an 83.4% approval, above the 75% minimum approval threshold. There were still approximately 3,076 unique comments, which were to be individually examined for incorporation into the next revision of draft 2.

June 25, 2007

The Wi-Fi Alliance announced its official certification program for devices based on draft 2.0.

September 7, 2007

Task Group agreed on all outstanding issues for draft 2.07. Draft 3.0 is authorized, with the expectation that it go to a sponsor ballot in November 2007.

November 2007

Draft 3.0 approved (240 voted affirmative, 43 negative, and 27 abstained). The editor was authorized to produce draft 3.01.

January 2008

Draft 3.02 approved. This version incorporates previously approved technical and editorial comments. There remain 127 unresolved technical comments. It was expected that all remaining comments will be resolved and that TGn and WG11 would subsequently release draft 4.0 for working group recirculation ballot following the March meeting.

May 2008

Draft 4.0 approved.

July 2008

Draft 5.0 approved and anticipated publication timeline modified.

September 2008

Draft 6.0 approved.

November 2008

Draft 7.0 approved.

January 2009

Draft 7.0 forwarded to sponsor ballot; the sponsor ballot was approved (158 for, 45 against, 21 abstaining); 241 comments were received.

March 2009

Draft 8.0 proceeded to sponsor ballot recirculation; the ballot passed by an 80.1% majority (75% required) (228 votes received, 169 approve, 42 not approve); 277 members are in the sponsor ballot pool; The comment resolution committee resolved the 77 comments received, and authorized the editor to create a draft 9.0 for further balloting.

April 4, 2009

Draft 9.0 passed sponsor ballot recirculation; the ballot passed by an 80.7% majority (75% required) (233 votes received, 171 approve, 41 not approve); 277 members are in the sponsor ballot pool; The comment resolution committee is resolving the 23 new comments received, and will authorize the editor to create a new draft for further balloting.

May 15, 2009

Draft 10.0 passed sponsor ballot recirculation

June 23, 2009

Draft 11.0 passed sponsor ballot recirculation

July 17, 2009

Final WG Approval passed with 53 approve, 1 against, 6 abstain.<sup>[16]</sup> Unanimous approval to send Final WG draft 11.0 to RevCom.<sup>[17]</sup>

September 11, 2009

RevCom/Standards Board approval.<sup>[18]</sup>

October 29, 2009

Published.<sup>[2]</sup>

## Comparison

802.11 network standards										
802.11 protocol	Release <sup>[19]</sup>	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream <sup>[20]</sup> (Mbit/s)	Allowable MIMO streams	Modulation	Approximate indoor range		Approximate outdoor range	
							(m)	(ft)	(m)	(ft)
—	Jun 1997	2.4	20	1, 2	1	DSSS, FHSS	20	unknown operator: u'strong'	100	unknown operator: u'strong'
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM	35	unknown operator: u'strong'	120	unknown operator: u'strong'
		3.7 <sup>[A]</sup>					—	—	5000	unknown operator: u'strong' <sup>[A]</sup>
b	Sep 1999	2.4	20	1, 2, 5.5, 11	1	DSSS	35	unknown operator: u'strong'	140	unknown operator: u'strong'

g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS	38	unknown operator: u'strong'	140	unknown operator: u'strong'
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 <sup>[B]</sup>	4	OFDM	70	unknown operator: u'strong'	250	unknown operator: u'strong' <sup>[21]</sup>
			40	15, 30, 45, 60, 90, 120, 135, 150 <sup>[B]</sup>			70	unknown operator: u'strong'	250	unknown operator: u'strong' <sup>[21]</sup>
ac (DRAFT)	Nov. 2011	5	20	up to 87.6 <sup>[22]</sup>	8					
			40	up to 200 <sup>[22]</sup>						
			80	up to 433.3 <sup>[22]</sup>						
			160	up to 866.7 <sup>[22]</sup>						

- A<sup>1</sup> A<sup>2</sup> IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5,000 m. As of 2009, it is only being licensed in the United States by the FCC.
- B<sup>1</sup> B<sup>2</sup> Assumes short guard interval (SGI) enabled, otherwise reduce each data rate by 10%.

## Standard

- *IEEE 802.11n-2009—Amendment 5: Enhancements for Higher Throughput*. IEEE-SA. 29 October 2009.  
doi:10.1109/IEEESTD.2009.5307322.
- IEEE 802.11n-2009<sup>[23]</sup>

## References

- [1] Stanford, Michael (September 7, 2007). "How does 802.11n get to 600Mbps?" (<http://www.wirevolution.com/2007/09/07/how-does-80211n-get-to-600mbps>). *Wirevolution*..
- [2] *IEEE 802.11n-2009—Amendment 5: Enhancements for Higher Throughput*. IEEE-SA. 29 October 2009.  
doi:10.1109/IEEESTD.2009.5307322.
- [3] <https://mentor.ieee.org/802.11/dcn/09/11-09-0576-03-000n-sp2-40mhz-coexistence-cids-presentation.ppt>
- [4] Wireless Without Compromise: Delivering the promise of IEEE 802.11n ([http://www.merunetworks.com/pdf/whitepapers/WP\\_80211nAppDelivery\\_v1.pdf](http://www.merunetworks.com/pdf/whitepapers/WP_80211nAppDelivery_v1.pdf))
- [5] Intel Ultimate N Wifi Link 5300 Product Brief (<http://download.intel.com/network/connectivity/products/wireless/319982.pdf>) (PDF)
- [6] <http://www.airmagnet.com/assets/whitepaper/WP-802.11nPrimer.pdf>
- [7] "How to: Minimize 802.11 Interference Issues" ([http://www.wireless-nets.com/resources/tutorials/minimize\\_802.11\\_interference\\_issues.html](http://www.wireless-nets.com/resources/tutorials/minimize_802.11_interference_issues.html)) . Retrieved 2008-07-30.
- [8] "How to: Migrate to 802.11n in the Enterprise" ([http://www.wireless-nets.com/resources/tutorials/migrate\\_80211n.html](http://www.wireless-nets.com/resources/tutorials/migrate_80211n.html)) . Retrieved 2008-07-30.
- [9] Shawn M. Jackman; Matt Swartz, Marcus Burton, Thomas W. Head (2011). *Certified Wireless Design Professional Official Study Guide* ([http://books.google.com/books?id=1yFnDbf\\_oMC&printsec=frontcover&dq=Certified+Wireless+Design+Professional+Official+Study+Guide&hl=en&sa=X&ei=r5E7T9f4MsHa4QSYjeWIBg&ved=0CDgQ6AEwAA](http://books.google.com/books?id=1yFnDbf_oMC&printsec=frontcover&dq=Certified+Wireless+Design+Professional+Official+Study+Guide&hl=en&sa=X&ei=r5E7T9f4MsHa4QSYjeWIBg&ved=0CDgQ6AEwAA)). John Wiley & Sons. pp. 519–521. ISBN 978-0470769041. .
- [10] Example: Channel 3 SCA (secondary channel above) also known as 3+7 reserves the first 9 out of the 11 channels available in North America.
- [11] "Wi-Fi Alliance Begins Testing of Next-Generation Wi-Fi Gear" ([http://www.wi-fi.org/pressroom\\_overview.php?newsid=574](http://www.wi-fi.org/pressroom_overview.php?newsid=574)). .
- [12] Wi-Fi Alliance Reveals New Logo and Announces First Wi-Fi CERTIFIED 802.11n draft 2.0 Products and Test Suite ([http://www.wi-fi.org/pressroom\\_overview.php?newsid=545](http://www.wi-fi.org/pressroom_overview.php?newsid=545)). *wi-fi.org*. May 16, 2007.
- [13] "WiFi Certified 802.11n draft 2.0 products" ([http://certifications.wi-fi.org/wbcs\\_certified\\_products.php?search=1&advanced=1&lang=en&filter\\_company\\_id=&filter\\_category\\_id=&filter\\_subcategory=&filter\\_cid=&date\\_from=&date\\_to=&x=30&y=18&selected\\_certifications\[\]](http://certifications.wi-fi.org/wbcs_certified_products.php?search=1&advanced=1&lang=en&filter_company_id=&filter_category_id=&filter_subcategory=&filter_cid=&date_from=&date_to=&x=30&y=18&selected_certifications[])). . Retrieved 2008-07-18.

- [14] "Wi-Fi Alliance launches updated Wi-Fi CERTIFIED n program" ([http://www.wi-fi.org/news\\_articles.php?f=media\\_news&news\\_id=892](http://www.wi-fi.org/news_articles.php?f=media_news&news_id=892)) (Press release). Wi-Fi Alliance. September 30, 2009..
- [15] "IEEE 802.11n Report (Status of Project)" ([http://grouper.ieee.org/groups/802/11/Reports/tgn\\_update.htm](http://grouper.ieee.org/groups/802/11/Reports/tgn_update.htm)). March 16, 2009. .
- [16] <https://mentor.ieee.org/802.11/dcn/09/11-09-0905-03-0000-july-2009-plenary-presentation-from-wg11-to-802-ec.ppt&nbsp;>;— Powerpoint Slide 10
- [17] "July 2009 meeting minutes" (<http://www.ieee802.org/minutes/2009-July/20090717-closing-minutes-v0.pdf>) (PDF). *IEEE 802 LMSC Executive Committee*. 17 July 2009. . Retrieved 10 August 2009.
- [18] "IEEE-SA - News & Events" ([http://standards.ieee.org/announcements/ieee802.11n\\_2009amendment\\_ratified.html](http://standards.ieee.org/announcements/ieee802.11n_2009amendment_ratified.html)). Standards.ieee.org. . Retrieved 2012-05-24.
- [19] "Official IEEE 802.11 working group project timelines" ([http://grouper.ieee.org/groups/802/11/Reports/802.11\\_Timelines.htm](http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm)). Sept. 19, 2009. . Retrieved 2009-10-09.
- [20] "Wi-Fi CERTIFIED n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi® Networks" ([http://www.wi-fi.org/register.php?file=wp\\_Wi-Fi\\_CERTIFIED\\_n\\_Industry.pdf](http://www.wi-fi.org/register.php?file=wp_Wi-Fi_CERTIFIED_n_Industry.pdf)) (registration required). *Wi-Fi Alliance*. September 2009. .
- [21] "802.11n Delivers Better Range" (<http://www.wi-fiplanet.com/tutorials/article.php/3680781>). *Wi-Fi Planet*. 2007-05-31. .
- [22] "IEEE802.11ac: The Next Evolution of Wi-Fi Standards" (<http://www.qualcomm.com/media/documents/files/ieee802-11ac-the-next-evolution-of-wi-fi.pdf>). 2012-05-11. . Retrieved 2012-05-16.
- [23] <http://standards.ieee.org/getieee802/download/802.11n-2009.pdf>

## **Resources (White papers, technical papers, application notes)**

- WLAN 802.11n - From SISO to MIMO (<http://www.rohde-schwarz.com/appnote/1MA179.pdf>)

# Other

## Twisted pair

**Twisted pair** cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs. It was invented by Alexander Graham Bell.

### Explanation

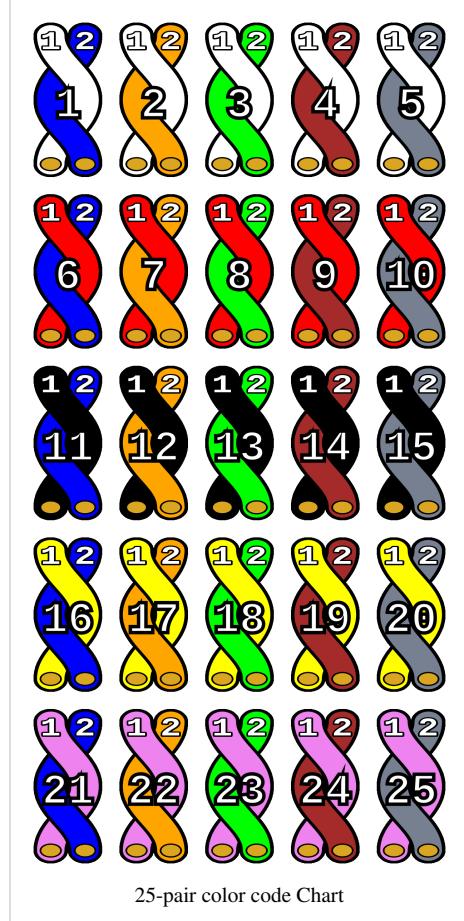
In balanced pair operation, the two wires carry equal and opposite signals and the destination detects the difference between the two. This is known as differential mode transmission. Noise sources introduce signals into the wires by coupling of electric or magnetic fields and tend to couple to both wires equally. The noise thus produces a common-mode signal which is cancelled at the receiver when the difference signal is taken.

This method starts to fail when the noise source is close to the signal wires; the closer wire will couple with the noise more strongly and the common-mode rejection of the receiver will fail to eliminate it. This problem is especially apparent in telecommunication cables where pairs in the same cable lie next to each other for many miles. One pair can induce crosstalk in another and it is additive along the length of the cable. Twisting the pairs counters this effect as on each half twist the wire nearest to the noise-source is exchanged.

Providing the interfering source remains uniform, or nearly so, over the distance of a single twist, the induced noise will remain common-mode. Differential signaling also reduces electromagnetic radiation from the cable, along with the associated attenuation allowing for greater distance between exchanges.

The twist rate (also called *pitch* of the twist, usually defined in twists per meter) makes up part of the specification for a given type of cable. Where nearby pairs have equal twist rates, the same conductors of the different pairs may repeatedly lie next to each other, partially undoing the benefits of differential mode. For this reason it is commonly specified that, at least for cables containing small numbers of pairs, the twist rates must differ.<sup>[1]</sup>

In contrast to **FTP** (foiled twisted pair) and **STP** (shielded twisted pair) cabling, **UTP** (unshielded twisted pair) cable is not surrounded by any shielding. It is the primary wire type for telephone usage and is very common for computer networking, especially as patch cables or temporary network connections due to the high flexibility of the cables.



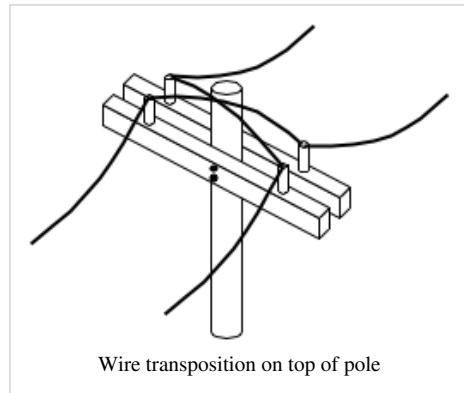
## History

The earliest telephones used telegraph lines, or open-wire single-wire earth return circuits. In the 1880s electric trams were installed in many cities, which induced noise into these circuits. Lawsuits being unavailing, the telephone companies converted to balanced circuits, which had the incidental benefit of reducing attenuation, hence increasing range.

As electrical power distribution became more commonplace, this measure proved inadequate. Two wires, strung on either side of cross bars on utility poles, shared the route with electrical power lines. Within a few years, the growing use of electricity again brought an increase of interference, so engineers devised a method called wire transposition, to cancel out the interference.

In wire transposition, the wires exchange position once every several poles. In this way, the two wires would receive similar EMI from power lines. This represented an early implementation of twisting, with a twist rate of about four twists per kilometre, or six per mile. Such open-wire balanced lines with periodic transpositions still survive today in some rural areas.

Twisted pair cables were invented by Alexander Graham Bell in 1881.<sup>[2]</sup> By 1900, the entire American telephone line network was either twisted pair or open wire with transposition to guard against interference. Today, most of the millions of kilometres of twisted pairs in the world are outdoor landlines, owned by telephone companies, used for voice service, and only handled or even seen by telephone workers.

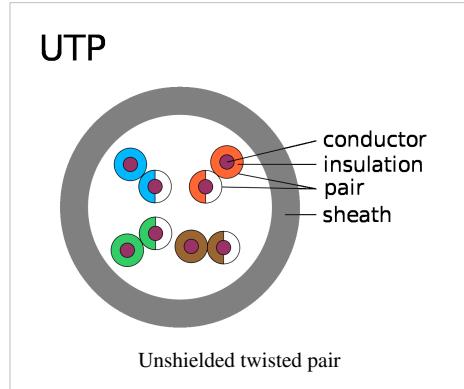


Wire transposition on top of pole

## Unshielded twisted pair (UTP)

UTP cables are found in many Ethernet networks and telephone systems. For indoor telephone applications, UTP is often grouped into sets of 25 pairs according to a standard 25-pair color code originally developed by AT&T. A typical subset of these colors (white/blue, blue/white, white/orange, orange/white) shows up in most UTP cables.

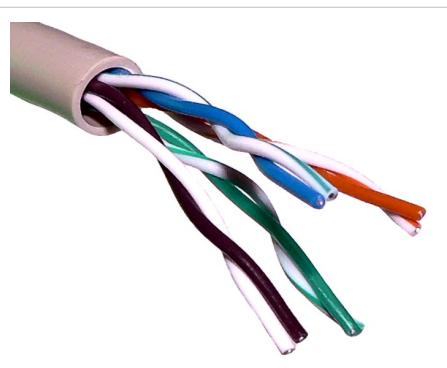
For urban outdoor telephone cables containing hundreds or thousands of pairs, the cable is divided into smaller but identical bundles. Each bundle consists of twisted pairs that have different twist rates. The bundles are in turn twisted together to make up the cable. Pairs having the same twist rate within the cable can still experience some degree of crosstalk. Wire pairs are selected carefully to minimize crosstalk within a large cable.



Unshielded twisted pair

UTP cable is also the most common cable used in computer networking. Modern Ethernet, the most common data networking standard, utilizes UTP cables. Twisted pair cabling is often used in data networks for short and medium length connections because of its relatively lower costs compared to optical fiber and coaxial cable.

UTP is also finding increasing use in video applications, primarily in security cameras. Many cameras include a UTP output with screw terminals; UTP cable bandwidth has improved to match the baseband of television signals. As UTP is a balanced transmission line, a balun is needed to connect to unbalanced equipment, for example any using BNC connectors and designed for coaxial cable.



Unshielded twisted pair cable with different twist rates

## Cable shielding

Twisted pair cables are often shielded in an attempt to prevent electromagnetic interference. Because the shielding is made of metal, it may also serve as a ground. However, usually a shielded or a screened twisted pair cable has a special grounding wire added called a drain wire.

This shielding can be applied to individual pairs, or to the collection of pairs. When shielding is applied to the collection of pairs, this is referred to as screening. Shielding provides an electric conductive barrier to attenuate electromagnetic waves external to the shield and provides conduction path by which induced currents can be circulated and returned to the source, via ground reference connection.

### Shielded twisted pair (STP or STP-A)

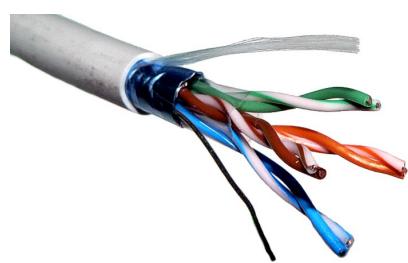
150 ohm STP shielded twisted pair cable is defined by the IBM Cabling System specifications and is used with token ring or FDDI networks. This type of shielding protects cable from external EMI from entering or exiting the cable and also protects neighboring pairs from crosstalk.

### Screened twisted pair (ScTP or F/TP)

ScTP cabling offers an overall sheath shield across all of the pairs within the 100 Ohm<sup>[3]</sup> twisted pair cable. F/TP uses foil shielding instead of a braided screen. This type of shielding protects EMI from entering or exiting the cable.

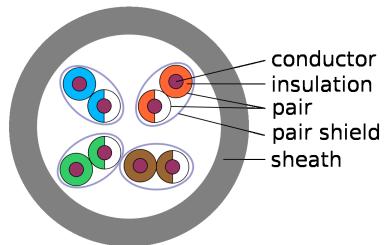
### Screened shielded twisted pair (S/STP or S/FTP)

S/STP (Screened Shielded Twisted Pair) or S/FTP (Screened Foiled Twisted Pair) cabling offer shielding between the pair sets and an overall sheath shield within the 100 Ohm twisted pair cable. This type of shielding protects EMI from entering or exiting the cable and also protects neighboring pairs from crosstalk.



ScTP, also known as FTP

## STP



STP cable format



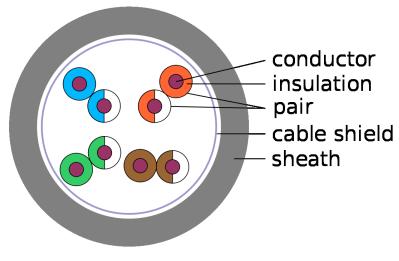
S-STP, also known as S/FTP.

S/STP cable<sup>[4]</sup> is both individually shielded (like STP cabling) and also has an outer metal shielding covering the entire group of shielded copper pairs (like S/UTP). This type of cabling offers the best protection from interference from external sources, and also eliminates *alien crosstalk*.<sup>[4]</sup>

Note that different vendors and authors use different terminology (i.e. STP has been used to denote both STP-A, S/STP, and S/UTP).<sup>[3]</sup> See below for the ISO/IEC attempt to internationally standardise the various designations.

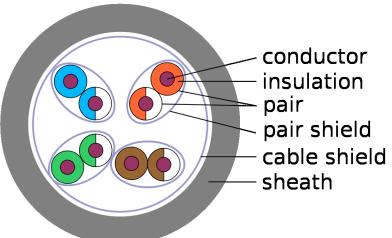
#### Comparison of some old and new abbreviations, according to ISO/IEC 11801:

**S/UTP**



S/UTP cable format

**S/STP**



S/STP cable format

Old name	New name	cable screening	pair shielding
UTP	U/UTP	none	none
STP	U/FTP	none	foil
FTP	F/UTP	foil	none
S-STP	S/FTP	braiding	foil
S-FTP	SF/UTP	foil, braiding	none

The code before the slash designates the shielding for the cable itself, while the code after the slash determines the shielding for the individual pairs:

TP = twisted pair

U = unshielded

F = foil shielding

S = braided shielding

## Most common twisted-pair cables

Name	Type	Bandwidth	Applications	Notes
Level 1		0.4 MHz	Telephone and modem lines	Not described in EIA/TIA recommendations. Unsuitable for modern systems. <sup>[5]</sup>
Level 2		4 MHz	Older terminal systems, e.g. IBM 3270	Not described in EIA/TIA recommendations. Unsuitable for modern systems. <sup>[5]</sup>
Cat3	UTP <sup>[6]</sup>	16 MHz <sup>[6]</sup>	10BASE-T and 100BASE-T4 Ethernet <sup>[6]</sup>	Described in EIA/TIA-568. Unsuitable for speeds above 16 Mbit/s. Now mainly for telephone cables <sup>[6]</sup>
Cat4	UTP <sup>[6]</sup>	20 MHz <sup>[6]</sup>	16 Mbit/s <sup>[6]</sup> Token Ring	Not commonly used <sup>[6]</sup>
Cat5	UTP <sup>[6]</sup>	100 MHz <sup>[6]</sup>	100BASE-TX & 1000BASE-T Ethernet <sup>[6]</sup>	Common in most current LANs <sup>[6]</sup>
Cat5e	UTP <sup>[6]</sup>	100 MHz <sup>[6]</sup>	100BASE-TX & 1000BASE-T Ethernet <sup>[6]</sup>	Enhanced Cat5. Same construction as Cat5, but with better testing standards.
Cat6	UTP <sup>[6]</sup>	250 MHz <sup>[6]</sup>	10GBASE-T Ethernet	Most commonly installed cable in Finland according to the 2002 standard. SFS-EN 50173-1
Cat6a		500 MHz	10GBASE-T Ethernet	ISO/IEC 11801:2002 Amendment 2.
Class F	S/FTP <sup>[6]</sup>	600 MHz <sup>[6]</sup>	Telephone, CCTV, 1000BASE-TX in the same cable. 10GBASE-T Ethernet.	Four pairs, S/FTP (shielded pairs, braid-screened cable). Development complete - ISO/IEC 11801 2nd Ed.
Class Fa		1000 MHz	Telephone, CATV, 1000BASE-TX in the same cable. 10GBASE-T Ethernet.	Four pairs, S/FTP (shielded pairs, braid-screened cable). Development complete - ISO/IEC 11801 2nd Ed. Am. 2.

## Solid core cable vs stranded cable

A solid core cable uses one solid wire per conductor and in a four pair cable there would be a total of eight solid wires.<sup>[6]</sup> Stranded conductor uses multiple wires wrapped around each other in each conductor and in a four pair with seven strands per conductor cable, there would be a total of 56 wires (2 per pair x 4 pairs x 7 strands).<sup>[6]</sup>

Solid core cable is supposed to be used for permanently installed runs. It is less flexible than stranded cable and is more prone to failure if repeatedly flexed. Stranded cable is used for fly leads at patch panel and for connections from wall-ports to end devices, as it resists cracking of the conductors. Stranded core is generally more expensive than solid core.

Connectors need to be designed differently for solid core than for stranded. Use of a connector with the wrong cable type is likely to lead to unreliable cabling. Plugs designed for solid and stranded core are readily available, and some vendors even offer plugs designed for use with both types. The punch-down blocks on patch-panel and wall port jacks are designed for use with solid core cable.

## Advantages

- It is a thin, flexible cable that is easy to string between walls.
- More lines can be run through the same wiring ducts.
- UTP costs less per meter/foot than any other type of LAN cable.
- Electrical noise going into or coming from the cable can be prevented.<sup>[7]</sup>
- Cross-talk is minimized.<sup>[7]</sup>

## Disadvantages

- Twisted pair's susceptibility to electromagnetic interference greatly depends on the pair twisting schemes (usually patented by the manufacturers) staying intact during the installation. As a result, twisted pair cables usually have stringent requirements for maximum pulling tension as well as minimum bend radius. This relative fragility of twisted pair cables makes the installation practices an important part of ensuring the cable's performance.
- In video applications that send information across multiple parallel signal wires, twisted pair cabling can introduce signaling delays known as skew which results in subtle color defects and ghosting due to the image components not aligning correctly when recombined in the display device. The skew occurs because twisted pairs within the same cable often use a different number of twists per meter so as to prevent crosstalk between pairs with identical numbers of twists. The skew can be compensated by varying the length of pairs in the termination box, so as to introduce delay lines that take up the slack between shorter and longer pairs, though the precise lengths required are difficult to calculate and vary depending on the overall cable length.

## Minor twisted pair variants

### Loaded twisted pair

A twisted pair that has intentionally added inductance, formerly common practice on telecommunication lines. The added inductors are known as load coils and reduce attenuation for voiceband frequencies but increase it on higher frequencies. Load coils cause distortion in voiceband on very long lines.<sup>[8]</sup>. In this context a line without load coils is referred to as an unloaded line.

### Bonded twisted pair

A twisted pair variant in which the pairs are individually bonded to increase robustness of the cable. Pioneered by Belden, it means the electrical specifications of the cable are maintained despite rough handling.

### Twisted ribbon cable

A variant of standard ribbon cable in which adjacent pairs of conductors are bonded and twisted together. The twisted pairs are then lightly bonded to each other in a ribbon format. Periodically along the ribbon there are short sections with no twisting to enable connectors and PCB headers to be terminated using the usual ribbon cable IDC techniques.

## References

- [1] "Crosstalk dependence on number of turns/inch for twisted pair versions of the endcap umbilical cable" ([http://www.hep.ph.ic.ac.uk/~dmray/pdffiles/TP\\_umbilical\\_studies.pdf](http://www.hep.ph.ic.ac.uk/~dmray/pdffiles/TP_umbilical_studies.pdf))..
- [2] US 244426 (<http://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=US244426>), Bell, Alexander Graham, "Telephone-circuit", issued 1881. See also TIFF format scans for USPTO 00244426 (<http://patimg1.uspto.gov/.piw?Docid=00244426&idkey=NONE>)
- [3] Anitech Systems MP 4000 Manual ([http://www.anitech-systems.com/MP4000/manual/briefs/ICM-4020E\\_Hub\\_Switch\\_Route\\_Cable\\_BR120501.pdf](http://www.anitech-systems.com/MP4000/manual/briefs/ICM-4020E_Hub_Switch_Route_Cable_BR120501.pdf))
- [4] Grounding for Screened and Shielded Network Cabling - Siemon ([http://www.siemon.com/us/white\\_papers/06-07-20-grounding.asp](http://www.siemon.com/us/white_papers/06-07-20-grounding.asp))
- [5] "CCNA: Network Media Types" (<http://www.ciscopress.com/articles/article.asp?p=31276>). .
- [6] "Comparison between CAT5, CAT5e, CAT6, CAT7 Cables" (<http://discountcablesusa.com/ethernet-cables100.html>). .
- [7] "Twisted Pair Testing" ([http://www.cirris.com/testing/twisted\\_pair/twist.html](http://www.cirris.com/testing/twisted_pair/twist.html)). .
- [8] cisco.com: *Understanding Line Impairments* ([http://www.cisco.com/en/US/tech/tk801/tk36/technologies\\_tech\\_note09186a00800a8663.shtml](http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a00800a8663.shtml)), visited 2012-06-04

## External links

- Telecommunications Virtual Museum (<http://www.telcomhistory.org/vm/sciencePhonesWork.shtml>)
- Independent comparative study UTP vs. STP for 10GBase-T (<http://www.utp-vs-stp.com>)

# Optical fiber

An **optical fiber** (or **optical fibre**) is a flexible, transparent fiber made of glass (silica) or plastic, slightly thicker than a human hair. It functions as a waveguide, or "light pipe"<sup>[1]</sup> to transmit light between the two ends of the fiber.<sup>[2]</sup> The field of applied science and engineering concerned with the design and application of optical fibers is known as **fiber optics**. Optical fibers are widely used in fiber-optic communications, which permits transmission over longer distances and at higher bandwidths (data rates) than other forms of communication. Fibers are used instead of metal wires because signals travel along them with less loss and are also immune to electromagnetic interference. Fibers are also used for illumination, and are wrapped in bundles so that they may be used to carry images, thus allowing viewing in confined spaces. Specially designed fibers are used for a variety of other applications, including sensors and fiber lasers.

Optical fibers typically include a transparent core surrounded by a transparent cladding material with a lower index of refraction. Light is kept in the core by total internal reflection. This causes the fiber to act as a waveguide. Fibers that support many propagation paths or transverse modes are called multi-mode fibers (MMF), while those that only support a single mode are called single-mode fibers (SMF). Multi-mode fibers generally have a wider core diameter, and are used for short-distance communication links and for applications where high power must be transmitted. Single-mode fibers are used for most communication links longer than 1050 meters (**unknown operator: u'strong' ft**).

Joining lengths of optical fiber is more complex than joining electrical wire or cable. The ends of the fibers must be carefully cleaved, and then spliced together, either mechanically or by fusing them with heat. Special optical fiber connectors for removable connections are also available.



A bundle of optical fibers



A TOSLINK fiber optic audio cable being illuminated at one end

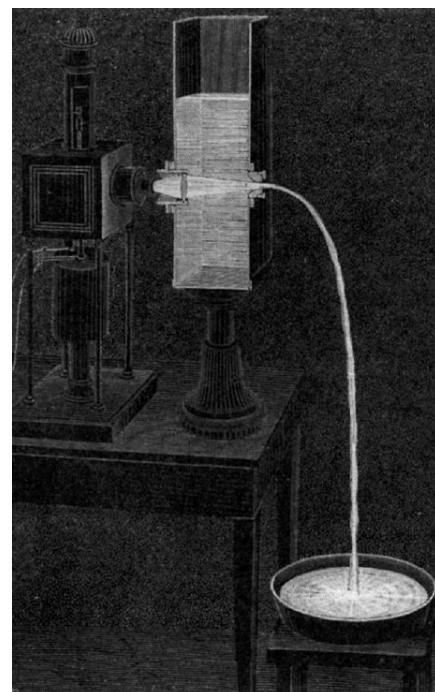


An optical fiber junction box. The yellow cables are single mode fibers; the orange and blue cables are multi-mode fibers: 50/125  $\mu\text{m}$  OM2 and 50/125  $\mu\text{m}$  OM3 fibers respectively.

## History

Fiber optics, though used extensively in the modern world, is a fairly simple, and relatively old, technology. Guiding of light by refraction, the principle that makes fiber optics possible, was first demonstrated by Daniel Colladon and Jacques Babinet in Paris in the early 1840s. John Tyndall included a demonstration of it in his public lectures in London, 12 years later.<sup>[3]</sup> Tyndall also wrote about the property of total internal reflection in an introductory book about the nature of light in 1870: "When the light passes from air into water, the refracted ray is bent *towards* the perpendicular... When the ray passes from water to air it is bent *from* the perpendicular... If the angle which the ray in water encloses with the perpendicular to the surface be greater than 48 degrees, the ray will not quit the water at all: it will be *totally reflected* at the surface.... The angle which marks the limit where total reflection begins is called the limiting angle of the medium. For water this angle is 48°27', for flint glass it is 38°41', while for diamond it is 23°42'."<sup>[4][5]</sup> Unpigmented human hairs have also been shown to act as an optical fiber.<sup>[6]</sup>

Practical applications, such as close internal illumination during dentistry, appeared early in the twentieth century. Image transmission through tubes was demonstrated independently by the radio experimenter Clarence Hansell and the television pioneer John Logie Baird in the 1920s. The principle was first used for internal medical examinations by Heinrich Lamm in the following decade. Modern optical fibers, where the glass fiber is coated with a transparent cladding to offer a more suitable refractive index,



Daniel Colladon first described this "light fountain" or "light pipe" in an 1842 article entitled *On the reflections of a ray of light inside a parabolic liquid stream*. This particular illustration comes from a later article by Colladon, in 1884.

appeared later in the decade.<sup>[3]</sup> Development then focused on fiber bundles for image transmission. Harold Hopkins and Narinder Singh Kapany at Imperial College in London achieved low-loss light transmission through a 75 cm long bundle which combined several thousand fibers. Their article titled "A flexible fibrescope, using static scanning" was published in the journal *Nature* in 1954.<sup>[7][8]</sup> The first fiber optic semi-flexible gastroscope was patented by Basil Hirschowitz, C. Wilbur Peters, and Lawrence E. Curtiss, researchers at the University of Michigan, in 1956. In the process of developing the gastroscope, Curtiss produced the first glass-clad fibers; previous optical fibers had relied on air or impractical oils and waxes as the low-index cladding material.

A variety of other image transmission applications soon followed.

In 1880 Alexander Graham Bell and Sumner Tainter invented the 'Photophone' at the Volta Laboratory in Washington, D.C., to transmit voice signals over an optical beam.<sup>[9]</sup> It was an advanced form of telecommunications, but subject to atmospheric interferences and impractical until the secure transport of light that would be offered by fiber-optical systems. In the late 19th and early 20th centuries, light was guided through bent glass rods to illuminate body cavities.<sup>[10]</sup> Jun-ichi Nishizawa, a Japanese scientist at Tohoku University, also proposed the use of optical fibers for communications in 1963, as stated in his book published in 2004 in India.<sup>[11]</sup> Nishizawa invented other technologies that contributed to the development of optical fiber communications, such as the graded-index optical fiber as a channel for transmitting light from semiconductor lasers.<sup>[12][13]</sup> The first working fiber-optical data transmission system was demonstrated by German physicist Manfred Börner at Telefunken Research Labs in Ulm in 1965, which was followed by the first patent application for this technology in 1966.<sup>[14][15]</sup> Charles K. Kao and George A. Hockham of the British company Standard Telephones and Cables (STC) were the first to promote the idea that the attenuation in optical fibers could be reduced below 20 decibels per kilometer (dB/km), making fibers a practical communication medium.<sup>[16]</sup> They proposed that the attenuation in fibers available at the time was caused by impurities that could be removed, rather than by fundamental physical effects such as scattering. They correctly and systematically theorized the light-loss properties for optical fiber, and pointed out the right material to use for such fibers — silica glass with high purity. This discovery earned Kao the Nobel Prize in Physics in 2009.<sup>[17]</sup>

NASA used fiber optics in the television cameras sent to the moon. At the time, the use in the cameras was classified *confidential*, and only those with the right security clearance or those accompanied by someone with the right security clearance were permitted to handle the cameras.<sup>[18]</sup>

The crucial attenuation limit of 20 dB/km was first achieved in 1970, by researchers Robert D. Maurer, Donald Keck, Peter C. Schultz, and Frank Zimar working for American glass maker Corning Glass Works, now Corning Incorporated. They demonstrated a fiber with 17 dB/km attenuation by doping silica glass with titanium. A few years later they produced a fiber with only 4 dB/km attenuation using germanium dioxide as the core dopant. Such low attenuation ushered in optical fiber telecommunication. In 1981, General Electric produced fused quartz ingots that could be drawn into fiber optic strands 25 miles (40 km) long.<sup>[19]</sup>

Attenuation in modern optical cables is far less than in electrical copper cables, leading to long-haul fiber connections with repeater distances of 70–150 kilometers (**unknown operator: u'strong'unknown operator: u'strong'unknown operator: u'strong' unknown operator: u'strong'**). The erbium-doped fiber amplifier, which reduced the cost of long-distance fiber systems by reducing or eliminating optical-electrical-optical repeaters, was co-developed by teams led by David N. Payne of the University of Southampton and Emmanuel Desurvire at Bell Labs in 1986. Robust modern optical fiber uses glass for both core and sheath, and is therefore less prone to aging. It was invented by Gerhard Bernsee of Schott Glass in Germany in 1973.<sup>[20]</sup>

The emerging field of photonic crystals led to the development in 1991 of photonic-crystal fiber,<sup>[21]</sup> which guides light by diffraction from a periodic structure, rather than by total internal reflection. The first photonic crystal fibers became commercially available in 2000.<sup>[22]</sup> Photonic crystal fibers can carry higher power than conventional fibers and their wavelength-dependent properties can be manipulated to improve performance.

## Applications

### Optical fiber communication

Optical fiber can be used as a medium for telecommunication and computer networking because it is flexible and can be bundled as cables. It is especially advantageous for long-distance communications, because light propagates through the fiber with little attenuation compared to electrical cables. This allows long distances to be spanned with few repeaters. Additionally, the per-channel light signals propagating in the fiber have been modulated at rates as high as 111 gigabits per second by NTT,<sup>[23][24]</sup> although 10 or 40 Gbit/s is typical in deployed systems.<sup>[25][26]</sup> Each fiber can carry many independent channels, each using a different wavelength of light (wavelength-division multiplexing (WDM)). The net data rate (data rate without overhead bytes) per fiber is the per-channel data rate reduced by the FEC overhead, multiplied by the number of channels (usually up to eighty in commercial dense WDM systems as of 2008). The current laboratory fiber optic data rate record, held by Bell Labs in Villarceaux, France, is multiplexing 155 channels, each carrying 100 Gbit/s over a 7000 km fiber.<sup>[27]</sup> Nippon Telegraph and Telephone Corporation has also managed 69.1 Tbit/s over a single 240 km fiber (multiplexing 432 channels, equating to 171 Gbit/s per channel).<sup>[28]</sup> Bell Labs also broke a 100 Petabit per second *kilometer* barrier (15.5 Tbit/s over a single 7000 km fiber).<sup>[29]</sup>

For short distance applications, such as a network in an office building, fiber-optic cabling can save space in cable ducts. This is because a single fiber can carry much more data than electrical cables such as standard category 5 Ethernet cabling, which typically runs at 100 Mbit/s or 1 Gbit/s speeds. Fiber is also immune to electrical interference; there is no cross-talk between signals in different cables, and no pickup of environmental noise. Non-armored fiber cables do not conduct electricity, which makes fiber a good solution for protecting communications equipment in high voltage environments, such as power generation facilities, or metal communication structures prone to lightning strikes. They can also be used in environments where explosive fumes are present, without danger of ignition. Wiretapping (in this case, fiber tapping) is more difficult compared to electrical connections, and there are concentric dual core fibers that are said to be tap-proof.<sup>[30]</sup>

### Fiber optic sensors

Fibers have many uses in remote sensing. In some applications, the sensor is itself an optical fiber. In other cases, fiber is used to connect a non-fiberoptic sensor to a measurement system. Depending on the application, fiber may be used because of its small size, or the fact that no electrical power is needed at the remote location, or because many sensors can be multiplexed along the length of a fiber by using different wavelengths of light for each sensor, or by sensing the time delay as light passes along the fiber through each sensor. Time delay can be determined using a device such as an *optical time-domain reflectometer*.

Optical fibers can be used as sensors to measure strain, temperature, pressure and other quantities by modifying a fiber so that the property to measure modulates the intensity, phase, polarization, wavelength, or transit time of light in the fiber. Sensors that vary the intensity of light are the simplest, since only a simple source and detector are required. A particularly useful feature of such fiber optic sensors is that they can, if required, provide distributed sensing over distances of up to one meter.

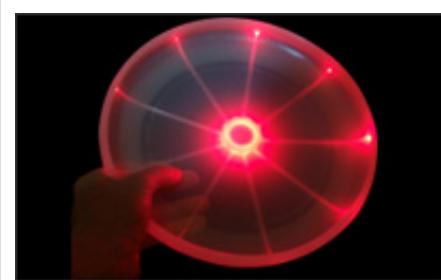
Extrinsic fiber optic sensors use an optical fiber cable, normally a multi-mode one, to transmit modulated light from either a non-fiber optical sensor—or an electronic sensor connected to an optical transmitter. A major benefit of extrinsic sensors is their ability to reach otherwise inaccessible places. An example is the measurement of temperature inside aircraft jet engines by using a fiber to transmit radiation into a radiation pyrometer outside the engine. Extrinsic sensors can be used in the same way to measure the internal temperature of electrical transformers, where the extreme electromagnetic fields present make other measurement techniques impossible. Extrinsic sensors measure vibration, rotation, displacement, velocity, acceleration, torque, and twisting. A solid state version of the gyroscope, using the interference of light, has been developed. The *fiber optic gyroscope (FOG)* has no moving

parts, and exploits the *Sagnac effect* to detect mechanical rotation.

Common uses for fiber optic sensors includes advanced intrusion detection security systems. The light is transmitted along a fiber optic sensor cable placed on a fence, pipeline, or communication cabling, and the returned signal is monitored and analysed for disturbances. This return signal is digitally processed to detect disturbances and trip an alarm if an intrusion has occurred.

## Other uses of optical fibers

Fibers are widely used in illumination applications. They are used as light guides in medical and other applications where bright light needs to be shone on a target without a clear line-of-sight path. In some buildings, optical fibers route sunlight from the roof to other parts of the building (see nonimaging optics). Optical fiber illumination is also used for decorative applications, including signs, art, toys and artificial Christmas trees. Swarovski boutiques use optical fibers to illuminate their crystal showcases from many different angles while only employing one light source. Optical fiber is an intrinsic part of the light-transmitting concrete building product, LiTraCon.



A frisbee illuminated by fiber optics

Optical fiber is also used in imaging optics. A coherent bundle of fibers is used, sometimes along with lenses, for a long, thin imaging device called an endoscope, which is used to view objects through a small hole. Medical endoscopes are used for minimally invasive exploratory or surgical procedures. Industrial endoscopes (see fiberscope or borescope) are used for inspecting anything hard to reach, such as jet engine interiors. Many microscopes use fiber-optic light sources to provide intense illumination of samples being studied.



Light reflected from optical fiber illuminates exhibited model

In spectroscopy, optical fiber bundles transmit light from a spectrometer to a substance that cannot be placed inside the spectrometer itself, in order to analyze its composition. A spectrometer analyzes substances by bouncing light off of and through them. By using fibers, a spectrometer can be used to study objects remotely.<sup>[31][32][33]</sup>

An optical fiber doped with certain rare earth elements such as erbium can be used as the gain medium of a laser or optical amplifier. Rare-earth doped optical fibers can be used to provide signal amplification by splicing a short section of doped fiber into a regular (undoped) optical fiber line. The doped fiber is optically pumped with a second laser wavelength that is coupled into the line in addition to the signal wave. Both wavelengths of light are transmitted through the doped fiber, which transfers energy from the second pump wavelength to the signal wave. The process that causes the amplification is stimulated emission.

Optical fibers doped with a wavelength shifter collect scintillation light in physics experiments.

Optical fiber can be used to supply a low level of power (around one watt) to electronics situated in a difficult electrical environment. Examples of this are electronics in high-powered antenna elements and measurement devices used in high voltage transmission equipment.

The iron sights for handguns, rifles, and shotguns may use short pieces of optical fiber for contrast enhancement.

## Principle of operation

An optical fiber is a cylindrical dielectric waveguide (nonconducting waveguide) that transmits light along its axis, by the process of total internal reflection. The fiber consists of a *core* surrounded by a cladding layer, both of which are made of dielectric materials. To confine the optical signal in the core, the refractive index of the core must be greater than that of the cladding. The boundary between the core and cladding may either be abrupt, in *step-index fiber*, or gradual, in *graded-index fiber*.



An overview of the operating principles of the optical fiber

## Index of refraction

The index of refraction is a way of measuring the speed of light in a material. Light travels fastest in a vacuum, such as outer space. The speed of light in a vacuum is about 300,000 kilometers (186,000 miles) per second. Index of refraction is calculated by dividing the speed of light in a vacuum by the speed of light in some other medium. The index of refraction of a vacuum is therefore 1, by definition. The typical value for the cladding of an optical fiber is 1.52.<sup>[34]</sup> The core value is typically 1.62.<sup>[34]</sup> The larger the index of refraction, the slower light travels in that medium. From this information, a good rule of thumb is that signal using optical fiber for communication will travel at around 200,000 kilometers per second. Or to put it another way, to travel 1000 kilometers in fiber, the signal will take 5 milliseconds to propagate. Thus a phone call carried by fiber between Sydney and New York, a 12,000-kilometer distance, means that there is an absolute minimum delay of 60 milliseconds (or around 1/16 of a second) between when one caller speaks to when the other hears. (Of course the fiber in this case will probably travel a longer route, and there will be additional delays due to communication equipment switching and the process of encoding and decoding the voice onto the fiber).

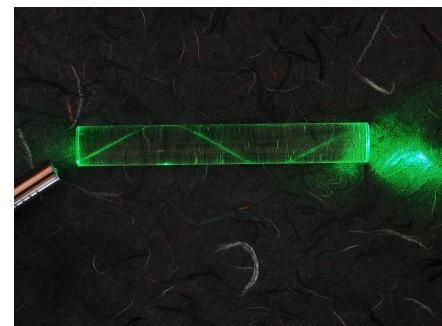
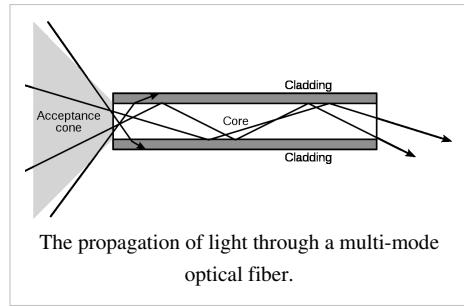
## Total internal reflection

When light traveling in an optically dense medium hits a boundary at a steep angle (larger than the critical angle for the boundary), the light will be completely reflected. This is called total internal reflection. This effect is used in optical fibers to confine light in the core. Light travels through the fiber core, bouncing back and forth off the boundary between the core and cladding. Because the light must strike the boundary with an angle greater than the critical angle, only light that enters the fiber within a certain range of angles can travel down the fiber without leaking out. This range of angles is called the acceptance cone of the fiber. The size of this acceptance cone is a function of the refractive index difference between the fiber's core and cladding.

In simpler terms, there is a maximum angle from the fiber axis at which light may enter the fiber so that it will propagate, or travel, in the core of the fiber. The sine of this maximum angle is the numerical aperture (NA) of the fiber. Fiber with a larger NA requires less precision to splice and work with than fiber with a smaller NA. Single-mode fiber has a small NA.

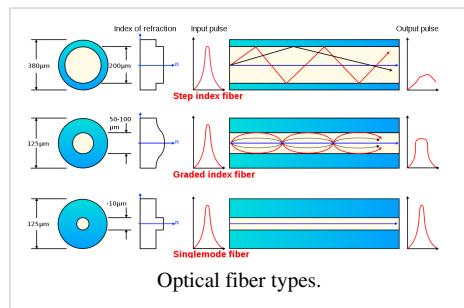
## Multi-mode fiber

Fiber with large core diameter (greater than 10 micrometers) may be analyzed by geometrical optics. Such fiber is called *multi-mode fiber*, from the electromagnetic analysis (see below). In a step-index multi-mode fiber, rays of light are guided along the fiber core by total internal reflection. Rays that meet the core-cladding boundary at a high angle (measured relative to a line normal to the boundary), greater than the critical angle for this boundary, are completely reflected. The critical angle (minimum angle for total internal reflection) is determined by the difference in index of refraction between the core and cladding materials. Rays that meet the boundary at a low angle are refracted from the core into the cladding, and do not convey light and hence information along the fiber. The critical angle determines the acceptance angle of the fiber, often reported as a numerical aperture. A high numerical aperture allows light to propagate down the fiber in rays both close to the axis and at various angles, allowing efficient coupling of light into the fiber. However, this high numerical aperture increases the amount of dispersion as rays at different angles have different path lengths and therefore take different times to traverse the fiber.



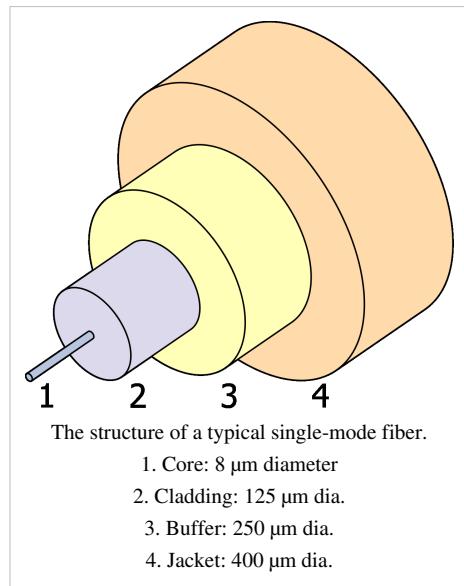
A laser bouncing down an acrylic rod, illustrating the total internal reflection of light in a multi-mode optical fiber.

In graded-index fiber, the index of refraction in the core decreases continuously between the axis and the cladding. This causes light rays to bend smoothly as they approach the cladding, rather than reflecting abruptly from the core-cladding boundary. The resulting curved paths reduce multi-path dispersion because high angle rays pass more through the lower-index periphery of the core, rather than the high-index center. The index profile is chosen to minimize the difference in axial propagation speeds of the various rays in the fiber. This ideal index profile is very close to a parabolic relationship between the index and the distance from the axis.



## Single-mode fiber

Fiber with a core diameter less than about ten times the wavelength of the propagating light cannot be modeled using geometric optics. Instead, it must be analyzed as an electromagnetic structure, by solution of Maxwell's equations as reduced to the electromagnetic wave equation. The electromagnetic analysis may also be required to understand behaviors such as speckle that occur when coherent light propagates in multi-mode fiber. As an optical waveguide, the fiber supports one or more confined transverse modes by which light can propagate along the fiber. Fiber supporting only one mode is called *single-mode* or *mono-mode fiber*. The behavior of larger-core multi-mode fiber can also be modeled using the wave equation, which shows that such fiber supports more than one mode of propagation (hence the name). The results of such modeling of multi-mode fiber approximately agree with the predictions of geometric optics, if the fiber core is large enough to support more than a few modes.



The waveguide analysis shows that the light energy in the fiber is not completely confined in the core. Instead, especially in single-mode fibers, a significant fraction of the energy in the bound mode travels in the cladding as an evanescent wave.

The most common type of single-mode fiber has a core diameter of 8–10 micrometers and is designed for use in the near infrared. The mode structure depends on the wavelength of the light used, so that this fiber actually supports a small number of additional modes at visible wavelengths. Multi-mode fiber, by comparison, is manufactured with core diameters as small as 50 micrometers and as large as hundreds of micrometers. The normalized frequency  $V$  for this fiber should be less than the first zero of the Bessel function  $J_0$  (approximately 2.405).

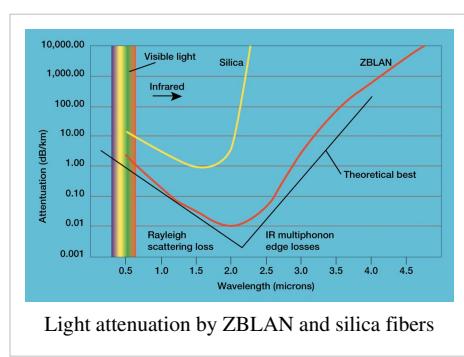
## Special-purpose fiber

Some special-purpose optical fiber is constructed with a non-cylindrical core and/or cladding layer, usually with an elliptical or rectangular cross-section. These include polarization-maintaining fiber and fiber designed to suppress whispering gallery mode propagation.

Photonic-crystal fiber is made with a regular pattern of index variation (often in the form of cylindrical holes that run along the length of the fiber). Such fiber uses diffraction effects instead of or in addition to total internal reflection, to confine light to the fiber's core. The properties of the fiber can be tailored to a wide variety of applications.

## Mechanisms of attenuation

Attenuation in fiber optics, also known as transmission loss, is the reduction in intensity of the light beam (or signal) with respect to distance traveled through a transmission medium. Attenuation coefficients in fiber optics usually use units of dB/km through the medium due to the relatively high quality of transparency of modern optical transmission media. The medium is usually a fiber of silica glass that confines the incident light beam to the inside. Attenuation is an important factor limiting the transmission of a digital signal across large distances. Thus, much research has gone into both limiting the



attenuation and maximizing the amplification of the optical signal. Empirical research has shown that attenuation in optical fiber is caused primarily by both scattering and absorption.

## Light scattering

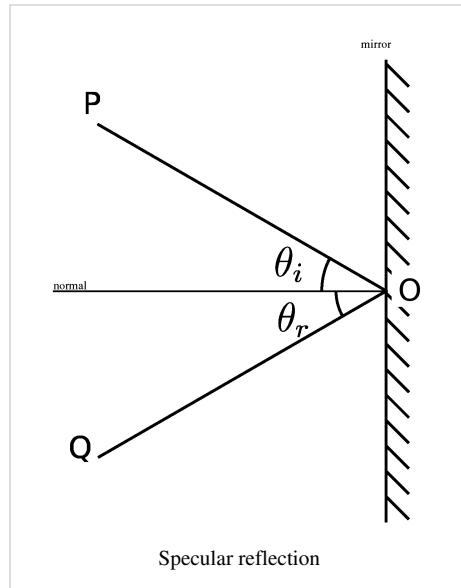
The propagation of light through the core of an optical fiber is based on total internal reflection of the lightwave. Rough and irregular surfaces, even at the molecular level, can cause light rays to be reflected in random directions. This is called diffuse reflection or scattering, and it is typically characterized by wide variety of reflection angles.

Light scattering depends on the wavelength of the light being scattered. Thus, limits to spatial scales of visibility arise, depending on the frequency of the incident light-wave and the physical dimension (or spatial scale) of the scattering center, which is typically in the form of some specific micro-structural feature. Since visible light has a wavelength of the order of one micrometer (one millionth of a meter) scattering centers will have dimensions on a similar spatial scale.

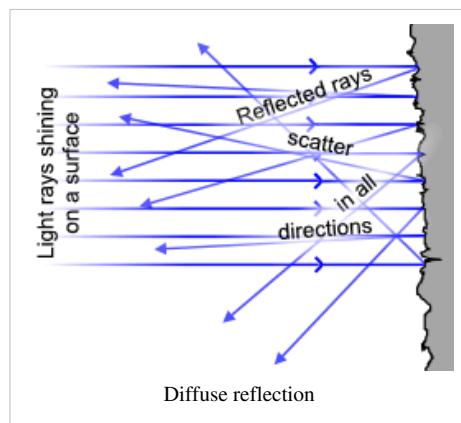
Thus, attenuation results from the incoherent scattering of light at internal surfaces and interfaces. In (poly)crystalline materials such as metals and ceramics, in addition to pores, most of the internal surfaces or interfaces are in the form of grain boundaries that separate tiny regions of crystalline order. It has recently been shown that when the size of the scattering center (or grain boundary) is reduced below the size of the wavelength of the light being scattered, the scattering no longer occurs to any significant extent. This phenomenon has given rise to the production of transparent ceramic materials.

Similarly, the scattering of light in optical quality glass fiber is caused by molecular level irregularities (compositional fluctuations) in the glass structure. Indeed, one emerging school of thought is that a glass is simply the limiting case of a polycrystalline solid. Within this framework, "domains" exhibiting various degrees of short-range order become the building blocks of both metals and alloys, as well as glasses and ceramics. Distributed both between and within these domains are micro-structural defects that provide the most ideal locations for light scattering. This same phenomenon is seen as one of the limiting factors in the transparency of IR missile domes.<sup>[35]</sup>

At high optical powers, scattering can also be caused by nonlinear optical processes in the fiber.<sup>[36][37]</sup>



Specular reflection



Diffuse reflection

## UV-Vis-IR absorption

In addition to light scattering, attenuation or signal loss can also occur due to selective absorption of specific wavelengths, in a manner similar to that responsible for the appearance of color. Primary material considerations include both electrons and molecules as follows:

- 1) At the electronic level, it depends on whether the electron orbitals are spaced (or "quantized") such that they can absorb a quantum of light (or photon) of a specific wavelength or frequency in the ultraviolet (UV) or visible ranges. This is what gives rise to color.
- 2) At the atomic or molecular level, it depends on the frequencies of atomic or molecular vibrations or chemical bonds, how close-packed its atoms or molecules are, and whether or not the atoms or molecules exhibit long-range order. These factors will determine the capacity of the material transmitting longer wavelengths in the infrared (IR),

far IR, radio and microwave ranges.

The design of any optically transparent device requires the selection of materials based upon knowledge of its properties and limitations. The Lattice absorption characteristics observed at the lower frequency regions (mid IR to far-infrared wavelength range) define the long-wavelength transparency limit of the material. They are the result of the interactive coupling between the motions of thermally induced vibrations of the constituent atoms and molecules of the solid lattice and the incident light wave radiation. Hence, all materials are bounded by limiting regions of absorption caused by atomic and molecular vibrations (bond-stretching) in the far-infrared ( $>10\text{ }\mu\text{m}$ ).

Thus, multi-phonon absorption occurs when two or more phonons simultaneously interact to produce electric dipole moments with which the incident radiation may couple. These dipoles can absorb energy from the incident radiation, reaching a maximum coupling with the radiation when the frequency is equal to the fundamental vibrational mode of the molecular dipole (e.g. Si-O bond) in the far-infrared, or one of its harmonics.

The selective absorption of infrared (IR) light by a particular material occurs because the selected frequency of the light wave matches the frequency (or an integer multiple of the frequency) at which the particles of that material vibrate. Since different atoms and molecules have different natural frequencies of vibration, they will selectively absorb different frequencies (or portions of the spectrum) of infrared (IR) light.

Reflection and transmission of light waves occur because the frequencies of the light waves do not match the natural resonant frequencies of vibration of the objects. When IR light of these frequencies strikes an object, the energy is either reflected or transmitted.

## Manufacturing

### Materials

Glass optical fibers are almost always made from silica, but some other materials, such as fluoro-zirconate, fluoroaluminate, and chalcogenide glasses as well as crystalline materials like sapphire, are used for longer-wavelength infrared or other specialized applications. Silica and fluoride glasses usually have refractive indices of about 1.5, but some materials such as the chalcogenides can have indices as high as 3. Typically the index difference between core and cladding is less than one percent.

Plastic optical fibers (POF) are commonly step-index multi-mode fibers with a core diameter of 0.5 millimeters or larger. POF typically have higher attenuation coefficients than glass fibers, 1 dB/m or higher, and this high attenuation limits the range of POF-based systems.

### Silica

Silica exhibits fairly good optical transmission over a wide range of wavelengths. In the near-infrared (near IR) portion of the spectrum, particularly around  $1.5\text{ }\mu\text{m}$ , silica can have extremely low absorption and scattering losses of the order of 0.2 dB/km. Such remarkably low losses are possible only because ultra-pure silicon is available, it being essential for manufacturing integrated circuits and discrete transistors. A high transparency in the  $1.4\text{-}\mu\text{m}$  region is achieved by maintaining a low concentration of hydroxyl groups (OH). Alternatively, a high OH concentration is better for transmission in the ultraviolet (UV) region.

Silica can be drawn into fibers at reasonably high temperatures, and has a fairly broad glass transformation range. One other advantage is that fusion splicing and cleaving of silica fibers is relatively effective. Silica fiber also has high mechanical strength against both pulling and even bending, provided that the fiber is not too thick and that the surfaces have been well prepared during processing. Even simple cleaving (breaking) of the ends of the fiber can provide nicely flat surfaces with acceptable optical quality. Silica is also relatively chemically inert. In particular, it is not hygroscopic (does not absorb water).

Silica glass can be doped with various materials. One purpose of doping is to raise the refractive index (e.g. with Germanium dioxide ( $\text{GeO}_2$ ) or Aluminium oxide ( $\text{Al}_2\text{O}_3$ )) or to lower it (e.g. with fluorine or Boron trioxide ( $\text{B}_2\text{O}_3$ )). Doping is also possible with laser-active ions (for example, rare earth-doped fibers) in order to obtain active fibers to be used, for example, in fiber amplifiers or laser applications. Both the fiber core and cladding are typically doped, so that the entire assembly (core and cladding) is effectively the same compound (e.g. an aluminosilicate, germanosilicate, phosphosilicate or borosilicate glass).

Particularly for active fibers, pure silica is usually not a very suitable host glass, because it exhibits a low solubility for rare earth ions. This can lead to quenching effects due to clustering of dopant ions. Aluminosilicates are much more effective in this respect.

Silica fiber also exhibits a high threshold for optical damage. This property ensures a low tendency for laser-induced breakdown. This is important for fiber amplifiers when utilized for the amplification of short pulses.

Because of these properties silica fibers are the material of choice in many optical applications, such as communications (except for very short distances with plastic optical fiber), fiber lasers, fiber amplifiers, and fiber-optic sensors. Large efforts put forth in the development of various types of silica fibers have further increased the performance of such fibers over other materials.<sup>[38][39][40][41][42][43][44][45]</sup>

## Fluorides

Fluoride glass is a class of non-oxide optical quality glasses composed of fluorides of various metals. Because of their low viscosity, it is very difficult to completely avoid crystallization while processing it through the glass transition (or drawing the fiber from the melt). Thus, although heavy metal fluoride glasses (HMFG) exhibit very low optical attenuation, they are not only difficult to manufacture, but are quite fragile, and have poor resistance to moisture and other environmental attacks. Their best attribute is that they lack the absorption band associated with the hydroxyl ( $\text{OH}$ ) group ( $3200\text{--}3600\text{ cm}^{-1}$ ), which is present in nearly all oxide-based glasses.

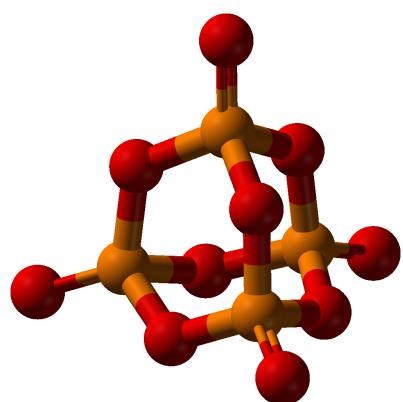
An example of a heavy metal fluoride glass is the ZBLAN glass group, composed of zirconium, barium, lanthanum, aluminium, and sodium fluorides. Their main technological application is as optical waveguides in both planar and fiber form. They are advantageous especially in the mid-infrared (2000–5000 nm) range.

HMGFs were initially slated for optical fiber applications, because the intrinsic losses of a mid-IR fiber could in principle be lower than those of silica fibers, which are transparent only up to about  $2\text{ }\mu\text{m}$ . However, such low losses were never realized in practice, and the fragility and high cost of fluoride fibers made them less than ideal as primary candidates. Later, the utility of fluoride fibers for various other applications was discovered. These include mid-IR spectroscopy, fiber optic sensors, thermometry, and imaging. Also, fluoride fibers can be used for guided lightwave transmission in media such as YAG (yttria-alumina garnet) lasers at  $2.9\text{ }\mu\text{m}$ , as required for medical applications (e.g. ophthalmology and dentistry).<sup>[46][47]</sup>

## Phosphates

Phosphate glass constitutes a class of optical glasses composed of metaphosphates of various metals. Instead of the  $\text{SiO}_4$  tetrahedra observed in silicate glasses, the building block for this glass former is Phosphorus pentoxide ( $\text{P}_2\text{O}_5$ ), which crystallizes in at least four different forms. The most familiar polymorph (see figure) comprises molecules of  $\text{P}_4\text{O}_{10}$ .

Phosphate glasses can be advantageous over silica glasses for optical fibers with a high concentration of doping rare earth ions. A mix of fluoride glass and phosphate glass is fluorophosphate glass.<sup>[48][49]</sup>



The  $\text{P}_4\text{O}_{10}$  cagelike structure—the basic building block for phosphate glass.

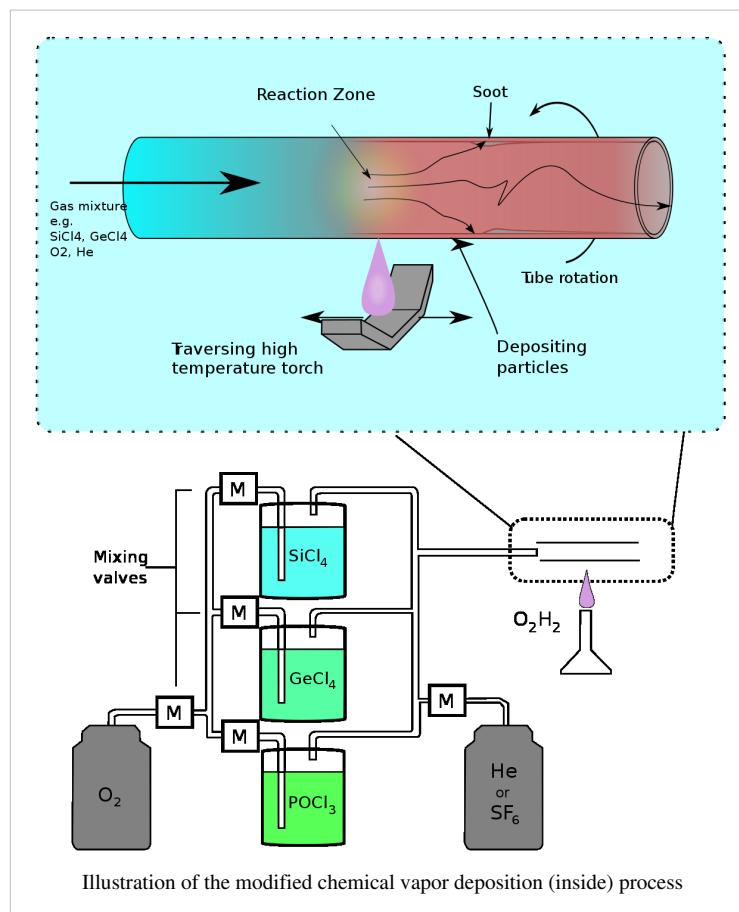
## Chalcogenides

The chalcogens—the elements in group 16 of the periodic table—particularly sulfur (S), selenium (Se) and tellurium (Te)—react with more electropositive elements, such as silver, to form chalcogenides. These are extremely versatile compounds, in that they can be crystalline or amorphous, metallic or semiconducting, and conductors of ions or electrons. Chalcogenides fibers are useful for far infrared transmission but are hard to produce.

## Process

Standard optical fibers are made by first constructing a large-diameter "preform", with a carefully controlled refractive index profile, and then "pulling" the preform to form the long, thin optical fiber. The preform is commonly made by three chemical vapor deposition methods: *inside vapor deposition*, *outside vapor deposition*, and *vapor axial deposition*.<sup>[50]</sup>

With *inside vapor deposition*, the preform starts as a hollow glass tube approximately 40 centimeters (**operator: u'strong' in**) long, which is placed horizontally and rotated slowly on a lathe. Gases such as silicon tetrachloride ( $\text{SiCl}_4$ ) or germanium tetrachloride ( $\text{GeCl}_4$ ) are injected with oxygen in the end of the tube. The gases are then heated by means of an external hydrogen burner, bringing the temperature of the gas up to 1900 K (1600 °C, 3000 °F), where the tetrachlorides react with oxygen to produce silica or germania (germanium dioxide) particles.



When the reaction conditions are chosen to allow this reaction to occur in the gas phase throughout the tube volume, in contrast to earlier techniques where the reaction occurred only on the glass surface, this technique is called *modified chemical vapor deposition (MCVD)*.

The oxide particles then agglomerate to form large particle chains, which subsequently deposit on the walls of the tube as soot. The deposition is due to the large difference in temperature between the gas core and the wall causing the gas to push the particles outwards (this is known as thermophoresis). The torch is then traversed up and down the length of the tube to deposit the material evenly. After the torch has reached the end of the tube, it is then brought back to the beginning of the tube and the deposited particles are then melted to form a solid layer. This process is repeated until a sufficient amount of material has been deposited. For each layer the composition can be modified by varying the gas composition, resulting in precise control of the finished fiber's optical properties.

In outside vapor deposition or vapor axial deposition, the glass is formed by *flame hydrolysis*, a reaction in which silicon tetrachloride and germanium tetrachloride are oxidized by reaction with water ( $H_2O$ ) in an oxyhydrogen flame. In outside vapor deposition the glass is deposited onto a solid rod, which is removed before further processing. In vapor axial deposition, a short *seed rod* is used, and a porous preform, whose length is not limited by the size of the source rod, is built up on its end. The porous preform is consolidated into a transparent, solid preform by heating to about 1800 K (1500 °C, 2800 °F).

The preform, however constructed, is then placed in a device known as a drawing tower, where the preform tip is heated and the optical fiber is pulled out as a string. By measuring the resultant fiber width, the tension on the fiber can be controlled to maintain the fiber thickness.

## Coatings

The light is "guided" down the core of the fiber by an optical "cladding" with a lower refractive index that traps light in the core through "total internal reflection."

The cladding is coated by a "buffer" that protects it from moisture and physical damage. The buffer is what gets stripped off the fiber for termination or splicing. These coatings are UV-cured urethane acrylate composite materials applied to the outside of the fiber during the drawing process. The coatings protect the very delicate strands of glass fiber—about the size of a human hair—and allow it to survive the rigors of manufacturing, proof testing, cabling and installation.

Today's glass optical fiber draw processes employ a dual-layer coating approach. An inner primary coating is designed to act as a shock absorber to minimize attenuation caused by microbending. An outer secondary coating protects the primary coating against mechanical damage and acts as a barrier to lateral forces. Sometimes a metallic armor layer is added to provide extra protection.

These fiber optic coating layers are applied during the fiber draw, at speeds approaching 100 kilometers per hour (**unknown operator: u'strong'** mph). Fiber optic coatings are applied using one of two methods: *wet-on-dry* and *wet-on-wet*. In wet-on-dry, the fiber passes through a primary coating application, which is then UV cured—then through the secondary coating application, which is subsequently cured. In wet-on-wet, the fiber passes through both the primary and secondary coating applications, then goes to UV curing.

Fiber optic coatings are applied in concentric layers to prevent damage to the fiber during the drawing application and to maximize fiber strength and microbend resistance. Unevenly coated fiber will experience non-uniform forces when the coating expands or contracts, and is susceptible to greater signal attenuation. Under proper drawing and coating processes, the coatings are concentric around the fiber, continuous over the length of the application and have constant thickness.

Fiber optic coatings protect the glass fibers from scratches that could lead to strength degradation. The combination of moisture and scratches accelerates the aging and deterioration of fiber strength. When fiber is subjected to low stresses over a long period, fiber fatigue can occur. Over time or in extreme conditions, these factors combine to

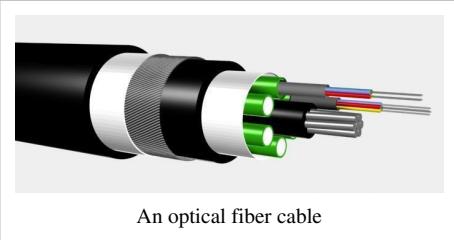
cause microscopic flaws in the glass fiber to propagate, which can ultimately result in fiber failure.

Three key characteristics of fiber optic waveguides can be affected by environmental conditions: strength, attenuation and resistance to losses caused by microbending. External fiber optic coatings protect glass optical fiber from environmental conditions that can affect the fiber's performance and long-term durability. On the inside, coatings ensure the reliability of the signal being carried and help minimize attenuation due to microbending.

## Practical issues

### Optical fiber cables

In practical fibers, the cladding is usually coated with a tough resin *buffer* layer, which may be further surrounded by a *jacket* layer, usually glass. These layers add strength to the fiber but do not contribute to its optical wave guide properties. Rigid fiber assemblies sometimes put light-absorbing ("dark") glass between the fibers, to prevent light that leaks out of one fiber from entering another. This reduces cross-talk between the fibers, or reduces flare in fiber bundle imaging applications.<sup>[51][52]</sup>



An optical fiber cable

Modern cables come in a wide variety of sheathings and armor, designed for applications such as direct burial in trenches, high voltage isolation, dual use as power lines,<sup>[53]</sup> installation in conduit, lashing to aerial telephone poles, submarine installation, and insertion in paved streets. The cost of small fiber-count pole-mounted cables has greatly decreased due to the high demand for fiber to the home (FTTH) installations in Japan and South Korea.

Fiber cable can be very flexible, but traditional fiber's loss increases greatly if the fiber is bent with a radius smaller than around 30 mm. This creates a problem when the cable is bent around corners or wound around a spool, making FTTX installations more complicated. "Bendable fibers", targeted towards easier installation in home environments, have been standardized as ITU-T G.657. This type of fiber can be bent with a radius as low as 7.5 mm without adverse impact. Even more bendable fibers have been developed.<sup>[54]</sup> Bendable fiber may also be resistant to fiber hacking, in which the signal in a fiber is surreptitiously monitored by bending the fiber and detecting the leakage.<sup>[55]</sup>

Another important feature of cable is cable's ability to withstand horizontally applied force. It is technically called max tensile strength defining how much force can be applied to the cable during the installation period.

Some fiber optic cable versions are reinforced with aramid yarns or glass yarns as intermediary strength member. In commercial terms, usage of the glass yarns are more cost effective while no loss in mechanical durability of the cable. Glass yarns also protect the cable core against rodents and termites.

## Termination and splicing

Optical fibers are connected to terminal equipment by optical fiber connectors. These connectors are usually of a standard type such as *FC*, *SC*, *ST*, *LC*, *MTRJ*, or *SMA*, which is designated for higher power transmission.

Optical fibers may be connected to each other by connectors or by *splicing*, that is, joining two fibers together to form a continuous optical waveguide. The generally accepted splicing method is arc fusion splicing, which melts the fiber ends together with an electric arc. For quicker fastening jobs, a “mechanical splice” is used.

Fusion splicing is done with a specialized instrument that typically operates as follows: The two cable ends are fastened inside a splice enclosure that will protect the splices, and the fiber ends are stripped of their protective polymer coating (as well as the more sturdy outer jacket, if present). The ends are *cleaved* (cut) with a precision cleaver to make them perpendicular, and are placed into special holders in the splicer. The splice is usually inspected via a magnified viewing screen to check the cleaves before and after the splice. The splicer uses small motors to align the end faces together, and emits a small spark between electrodes at the gap to burn off dust and moisture. Then the splicer generates a larger spark that raises the temperature above the melting point of the glass, fusing the ends together permanently. The location and energy of the spark is carefully controlled so that the molten core and cladding do not mix, and this minimizes optical loss. A splice loss estimate is measured by the splicer, by directing light through the cladding on one side and measuring the light leaking from the cladding on the other side. A splice loss under 0.1 dB is typical. The complexity of this process makes fiber splicing much more difficult than splicing copper wire.



ST connectors on multi-mode fiber.

Mechanical fiber splices are designed to be quicker and easier to install, but there is still the need for stripping, careful cleaning and precision cleaving. The fiber ends are aligned and held together by a precision-made sleeve, often using a clear index-matching gel that enhances the transmission of light across the joint. Such joints typically have higher optical loss and are less robust than fusion splices, especially if the gel is used. All splicing techniques involve installing an enclosure that protects the splice.

Fibers are terminated in connectors that hold the fiber end precisely and securely. A fiber-optic connector is basically a rigid cylindrical barrel surrounded by a sleeve that holds the barrel in its mating socket. The mating mechanism can be *push and click*, *turn and latch (bayonet)*, or *screw-in (threaded)*. A typical connector is installed by preparing the fiber end and inserting it into the rear of the connector body. Quick-set adhesive is usually used to hold the fiber securely, and a strain relief is secured to the rear. Once the adhesive sets, the fiber's end is polished to a mirror finish. Various polish profiles are used, depending on the type of fiber and the application. For single-mode fiber, fiber ends are typically polished with a slight curvature that makes the mated connectors touch only at their cores. This is called a *physical contact (PC)* polish. The curved surface may be polished at an angle, to make an *angled physical contact (APC)* connection. Such connections have higher loss than PC connections, but greatly reduced back reflection, because light that reflects from the angled surface leaks out of the fiber core. The resulting signal strength loss is called *gap loss*. APC fiber ends have low back reflection even when disconnected.

In the 1990s, terminating fiber optic cables was labor intensive. The number of parts per connector, polishing of the fibers, and the need to oven-bake the epoxy in each connector made terminating fiber optic cables difficult. Today, many connector types are on the market that offer easier, less labor intensive ways of terminating cables. Some of the most popular connectors are pre-polished at the factory, and include a gel inside the connector. Those two steps help save money on labor, especially on large projects. A cleave is made at a required length, to get as close to the polished piece already inside the connector. The gel surrounds the point where the two pieces meet inside the

connector for very little light loss.

## Free-space coupling

It is often necessary to align an optical fiber with another optical fiber, or with an optoelectronic device such as a light-emitting diode, a laser diode, or a modulator. This can involve either carefully aligning the fiber and placing it in contact with the device, or can use a lens to allow coupling over an air gap. In some cases the end of the fiber is polished into a curved form that makes it act as a lens. Some companies can even shape the fiber into lenses by cutting them with lasers<sup>[56]</sup>.

In a laboratory environment, a bare fiber end is coupled using a fiber launch system, which uses a microscope objective lens to focus the light down to a fine point. A precision translation stage (micro-positioning table) is used to move the lens, fiber, or device to allow the coupling efficiency to be optimized. Fibers with a connector on the end make this process much simpler: the connector is simply plugged into a pre-aligned fiberoptic collimator, which contains a lens that is either accurately positioned with respect to the fiber, or is adjustable. To achieve the best injection efficiency into single-mode fiber, the direction, position, size and divergence of the beam must all be optimized. With good beams, 70 to 90% coupling efficiency can be achieved.

With properly polished single-mode fibers, the emitted beam has an almost perfect Gaussian shape—even in the far field—if a good lens is used. The lens needs to be large enough to support the full numerical aperture of the fiber, and must not introduce aberrations in the beam. Aspheric lenses are typically used.

## Fiber fuse

At high optical intensities, above 2 megawatts per square centimeter, when a fiber is subjected to a shock or is otherwise suddenly damaged, a *fiber fuse* can occur. The reflection from the damage vaporizes the fiber immediately before the break, and this new defect remains reflective so that the damage propagates back toward the transmitter at 1–3 meters per second (4–11 km/h, 2–8 mph).<sup>[57][58]</sup> The open fiber control system, which ensures laser eye safety in the event of a broken fiber, can also effectively halt propagation of the fiber fuse.<sup>[59]</sup> In situations, such as undersea cables, where high power levels might be used without the need for open fiber control, a "fiber fuse" protection device at the transmitter can break the circuit to keep damage to a minimum.

## Example

Fiber connections can be used for various types of connections. For example, most high definition televisions offer a digital audio optical connection. This allows the streaming of audio over light, using the TOSLink protocol.

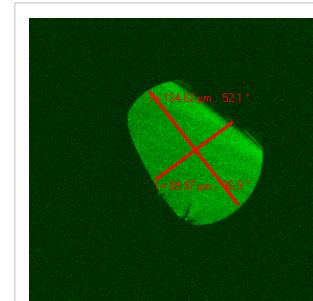
## Power transmission

Optical fiber can be used to transmit power using a photovoltaic cell to convert the light into electricity.<sup>[60]</sup> While this method of power transmission is not as efficient as conventional ones, it is especially useful in situations where it is desirable not to have a metallic conductor as in the case of use near MRI machines, which produce strong magnetic fields.<sup>[61]</sup>

## Preform

A preform is a piece of glass used to draw an optical fiber. The preform may consist of several pieces of a glass with different refractive indices, to provide the core and cladding of the fiber. The shape of the preform may be circular, although for some applications such as double-clad fibers another form is preferred.<sup>[62]</sup> In fiber lasers based on double-clad fiber, an asymmetric shape improves the filling factor for laser pumping.

Because of the surface tension, the shape is smoothed during the drawing process, and the shape of the resulting fiber does not reproduce the sharp edges of the preform. Nevertheless, the careful polishing of the **preform** is important, any defects of the **preform** surface affect the optical and mechanical properties of the resulting fiber. In particular, the preform for the test-fiber shown in the figure was not polished well, and the cracks are seen with confocal optical microscope.



Cross-section of a fiber drawn from a D-shaped **preform**

## References

- [1] Light Pipe (<http://www.catb.org/jargon/html/L/light-pipe.html>) entry at the Jargon File
- [2] K. Thyagarajan; Ajoy K. Ghatak (10 September 2007). *Fiber Optic Essentials* (<http://books.google.com/books?id=k83sN7SJLVgC&pg=PA34>). Wiley-Interscience. pp. 34–. ISBN 978-0-470-09742-7. . Retrieved 1 May 2012.
- [3] Bates, Regis J (2001). *Optical Switching and Networking Handbook*. New York: McGraw-Hill. p. 10. ISBN 0-07-137356-X.
- [4] Tyndall, John (1870). "Total Reflexion" (<http://www.archive.org/details/notesofcourseofn00tyndrich>). *Notes about Light*..
- [5] Tyndall, John (1873). "Six Lectures on Light" (<http://www.archive.org/details/sixlecturesonlig00tynduoft>). .
- [6] Wells, J. (1989). "Hair light guide". *Nature* **338** (6210): 23. Bibcode 1989Natur.338...23W. doi:10.1038/338023b0. PMID 2918918.
- [7] H. H. Hopkins and N. S. Kapany (1954). "A flexible fibrescope, using static scanning". *Nature* **173** (4392): 39. Bibcode 1954Natur.173...39H. doi:10.1038/173039b0.
- [8] Two Revolutionary Optical Technologies ([http://www.nobelprize.org/nobel\\_prizes/physics/laureates/2009/sciback\\_phy\\_09.pdf](http://www.nobelprize.org/nobel_prizes/physics/laureates/2009/sciback_phy_09.pdf)). Scientific Background on the Nobel Prize in Physics 2009. Nobelprize.org. 6 October 2009
- [9] Jones, Newell. First 'Radio' Built by San Diego Resident Partner of Inventor of Telephone: Keeps Notebook of Experiences With Bell (<http://history.sandiego.edu/gen/recording/ar304.html>), San Diego Evening Tribune, July 31, 1937. Retrieved from the University of San Diego History Department website, November 26, 2009.
- [10] The Birth of Fiber Optics (<http://inventors.about.com/library/weekly/aa980407.htm>)
- [11] Nishizawa, Jun-ichi and Suto, Ken (2004). "Terahertz wave generation and light amplification using Raman effect" (<http://books.google.com/?id=2NTpSnfhResC&pg=PA27>). In Bhat, K. N. and DasGupta, Amitava. *Physics of semiconductor devices*. New Delhi, India: Narosa Publishing House. p. 27. ISBN 81-7319-567-6. .
- [12] "Optical Fiber" (<http://www.city.sendai.jp/soumu/kouhou/s-new-e6/page01.html>). *Sendai New*.. Retrieved April 5, 2009.
- [13] "New Medal Honors Japanese Microelectronics Industry Leader" ([http://www.ieee.org/portal/site/tionline/menuitem.130a3558587d56e8fb2275875bac26c8/index.jsp?&pName=institute\\_level1\\_article&TheCat=1003&article=tionline/legacy/inst2003/jun03/6w.nishizawa.xml&](http://www.ieee.org/portal/site/tionline/menuitem.130a3558587d56e8fb2275875bac26c8/index.jsp?&pName=institute_level1_article&TheCat=1003&article=tionline/legacy/inst2003/jun03/6w.nishizawa.xml&)). *Institute of Electrical and Electronics Engineers*.
- [14] DE patent 1254513 (<http://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=DE1254513>), Dr. Manfred Börner, "Mehrstufiges Übertragungssystem für Pulscodemodulation dargestellte Nachrichten.", issued 1967-11-16, assigned to Telefunken Patentverwertungsgesellschaft m.b.H.
- [15] US patent 3845293 (<http://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=US3845293>), Manfred Börner, "Electro-optical transmission system utilizing lasers"
- [16] Hecht, Jeff (1999). *City of Light, The Story of Fiber Optics* (<http://books.google.com/?id=4oMu7RbGpqUC&pg=PA114>). New York: Oxford University Press. p. 114. ISBN 0-19-510818-3..
- [17] "Press Release — Nobel Prize in Physics 2009" ([http://nobelprize.org/nobel\\_prizes/physics/laureates/2009/press.html](http://nobelprize.org/nobel_prizes/physics/laureates/2009/press.html)). The Nobel Foundation. . Retrieved 2009-10-07.
- [18] Lunar Television Camera. Pre-installation Acceptance Test Plan (<http://history.nasa.gov/alsj/MSC-SESD-28-105.pdf>). NASA. 12 March 1968
- [19] "1971–1985 Continuing the Tradition" (<http://www.ge.com/innovation/timeline/index.html>). *GE Innovation Timeline*. General Electric Company. . Retrieved 2008-10-22.
- [20] U.S. Patent 3966300 (<http://www.google.com/patents?vid=3966300>) "Light conducting fibers of quartz glass"
- [21] Russell, Philip (2003). "Photonic Crystal Fibers". *Science* **299** (5605): 358–62. Bibcode 2003Sci...299..358R. doi:10.1126/science.1079280. PMID 12532007.

- [22] "The History of Crystal fiber A/S" (<http://www.crystal-fiber.com/>). Crystal Fiber A/S. . Retrieved 2008-10-22.
- [23] 14 Tbps over a Single Optical Fiber (<http://www.ntt.co.jp/news/news06e/0609/060929a.html>): Successful Demonstration of World's Largest Capacity – 145 digital high-definition movies transmitted in one second. NTT Press Release. September 29, 2006.
- [24] M. S. Alfiad, et al. (2008). "111 Gb/s POLMUX-RZ-DQPSK Transmission over 1140 km of SSMF with 10.7 Gb/s NRZ-OOK Neighbours". *Proceedings ECOC 2008*: pp. Mo.4.E.2.
- [25] S. Yao, "Polarization in Fiber Systems: Squeezing Out More Bandwidth" (<http://www.generalphotonics.com/pdf/PSReprint.pdf>), The Photonics Handbook, Laurin Publishing, 2003, p. 1.
- [26] Ciena, JANET Delivers Europe's First 40 Gbps Wavelength Service ([http://www.ciena.com/news/news\\_2007pr\\_6976.htm](http://www.ciena.com/news/news_2007pr_6976.htm)) 07/09/2007. Retrieved 29 Oct 2009.
- [27] !!!x-in-lab/ Alcatel Boosts Fiber Speed to 100 Petabits in Lab (<http://gigaom.com/2009/09/28/alcatel-lucent-boasts-fiber-speeds-by-10natas>), Stacey Higginbotham, Sep. 28, 2009
- [28] World Record 69-Terabit Capacity for Optical Transmission over a Single Optical Fiber (<http://www.ntt.co.jp/news2010/1003e/100325a.html>). NTT.co.jp. March 25, 2010
- [29] Bell Labs breaks optical transmission record, 100 Petabit per second kilometer barrier (<http://www.physorg.com/news173455192.html>). Physorg. September 29, 2009
- [30] Siemen's claim to a fiber optic line that can not be tapped ([http://www.automation.siemens.com/net/html\\_76/produkte/040\\_ie\\_fc\\_glasleitungen.htm](http://www.automation.siemens.com/net/html_76/produkte/040_ie_fc_glasleitungen.htm)). Retrieved 18 Dec 2009.
- [31] Al Mosheky, Zaid; Melling, Peter J. ; Thomson, Mary A. (June 2001). "In situ real-time monitoring of a fermentation reaction using a fiber-optic FT-IR probe" (<http://www.remspec.com/pdfs/SP5619.pdf>) (PDF). *Spectroscopy* . .
- [32] Melling, Peter; Thomson, Mary (October 2002). "Reaction monitoring in small reactors and tight spaces" (<http://www.remspec.com/pdfs/amlab1002.pdf>) (PDF). *American Laboratory News* . .
- [33] Melling, Peter J.; Thomson, Mary (2002). "Fiber-optic probes for mid-infrared spectrometry" ([http://www.remspec.com/pdfs/2703\\_o.pdf](http://www.remspec.com/pdfs/2703_o.pdf)). In Chalmers, John M.; Griffiths, Peter R. (eds.) (PDF). *Handbook of Vibrational Spectroscopy*. Wiley.. .
- [34] Eugene Hecht. Optics, 4th ed. San Francisco, USA: Pearson Education inc. 2002.
- [35] Archibald, P.S. and Bennett, H.E. (1978). "Scattering from infrared missile domes". *Opt. Engr.* **17**: 647.
- [36] Smith, R. G. (1972). "Optical Power Handling Capacity of Low Loss Optical Fibers as Determined by Stimulated Raman and Brillouin Scattering". *Applied Optics* **11** (11): 2489–94. Bibcode 1972ApOpt..11.2489S. doi:10.1364/AO.11.002489. PMID 20119362.
- [37] Paschotta, Rüdiger. "Brillouin Scattering" ([http://www.rp-photonics.com/brillouin\\_scattering.html](http://www.rp-photonics.com/brillouin_scattering.html)). *Encyclopedia of Laser Physics and Technology*. RP Photonics. .
- [38] Glasesmenn, G. S. (1999). "Advancements in Mechanical Strength and Reliability of Optical Fibers" (<http://www.corning.com/WorkArea/downloadasset.aspx?id=7783>). *Proc. SPIE CR73*: 1..
- [39] Kurkjian, Charles R.; Simpkins, Peter G.; Inniss, Daryl (1993). "Strength, Degradation, and Coating of Silica Lightguides". *Journal of the American Ceramic Society* **76** (5): 1106. doi:10.1111/j.1151-2916.1993.tb03727.x.
- [40] Kurkjian, C (1988). "Mechanical stability of oxide glasses". *Journal of Non-Crystalline Solids* **102**: 71. Bibcode 1988JNCS..102...71K. doi:10.1016/0022-3093(88)90114-7.
- [41] Kurkjian, C.R.; Krause, J.T.; Matthewson, M.J. (1989). "Strength and fatigue of silica optical fibers". *Journal of Lightwave Technology* **7** (9): 1360. Bibcode 1989JLwT....7.1360K. doi:10.1109/50.50715.
- [42] Kurkjian, Charles R. (1999). "Strength variations in silica fibers". *Proceedings of SPIE*. **3848**. p. 77. doi:10.1117/12.372757.
- [43] Skontorp, Arne (2000). "Nonlinear mechanical properties of silica-based optical fibers". *Proceedings of SPIE*. **4073**. p. 278. doi:10.1117/12.396408.
- [44] Proctor, B. A.; Whitney, I.; Johnson, J. W. (1967). "The Strength of Fused Silica". *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences (1934–1990)* **297** (1451): 534. Bibcode 1967RSPSA.297..534P. doi:10.1098/rspa.1967.0085.
- [45] Bartenev, G (1968). "The structure and strength of glass fibers". *Journal of Non-Crystalline Solids* **1**: 69. Bibcode 1968JNCS....1..69B. doi:10.1016/0022-3093(68)90007-0.
- [46] Tran, D., et al. (1984). "Heavy metal fluoride glasses and fibers: A review" ([http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?arnumber=1073661](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1073661)). *J. Lightwave Technology* **2** (5): 566. Bibcode 1984JLwT....2..566T. doi:10.1109/JLT.1984.1073661..
- [47] Nee, Soe-Mie F. (2000). "Optical and surface properties of oxyfluoride glass". *Proceedings of SPIE*. **4102**. p. 122. doi:10.1117/12.405276.
- [48] Karabulut, M (2001). "Mechanical and structural properties of phosphate glasses". *Journal of Non-Crystalline Solids* **288**: 8. Bibcode 2001JNCS..288....8K. doi:10.1016/S0022-3093(01)00615-9.
- [49] Kurkjian, C (2000). "Mechanical properties of phosphate glasses". *Journal of Non-Crystalline Solids* **263–264**: 207. Bibcode 2000JNCS..263..207K. doi:10.1016/S0022-3093(99)00637-7.
- [50] Gowar, John (1993) (2d ed.). Hempstead, UK: Prentice-Hall. p. 209. ISBN 0-13-638727-6.
- [51] "Light collection and propagation" (<http://zone.ni.com/devzone/cda/ph/p/id/129#toc2>). *National Instruments' Developer Zone*. National Instruments Corporation. . Retrieved 2007-03-19.
- [52] Hecht, Jeff (2002). *Understanding Fiber Optics* (4th ed.). Prentice Hall. ISBN 0-13-027828-9.
- [53] "Screening report for Alaska rural energy plan" ([http://web.archive.org/web/20060508191931/http://www.dced.state.ak.us/dca/AEIS/PDF\\_Files/AIDEA\\_Energy\\_Screening.pdf](http://web.archive.org/web/20060508191931/http://www.dced.state.ak.us/dca/AEIS/PDF_Files/AIDEA_Energy_Screening.pdf)) (PDF). *Alaska Division of Community and Regional Affairs*. Archived from the original ([http://www.dced.state.ak.us/dca/AEIS/PDF\\_Files/AIDEA\\_Energy\\_Screening.pdf](http://www.dced.state.ak.us/dca/AEIS/PDF_Files/AIDEA_Energy_Screening.pdf)) on May 8, 2006. . Retrieved April 11, 2006.

- [54] "Corning announces breakthrough optical fiber technology" ([http://www.corning.com/media\\_center/press\\_releases/2007/2007072301.aspx](http://www.corning.com/media_center/press_releases/2007/2007072301.aspx)) (Press release). Corning Incorporated. 2007-07-23. . Retrieved 2007-12-09.
- [55] Olzak, Tom (2007-05-03). "Protect your network against fiber hacks" (<http://blogs.techrepublic.com.com/security/?p=222>). *Techrepublic*. CNET. . Retrieved 2007-12-10.
- [56] "OpTek Systems Inc." (<http://www.opteksystems.com/laser-lens>). .
- [57] Atkins, R. M.; Simpkins, P. G.; Yablon, A. D. (2003). "Track of a fiber fuse: a Rayleigh instability in optical waveguides" (<http://ol.osa.org/abstract.cfm?id=72607>). *Optics Letters* **28** (12): 974–976. Bibcode 2003OptL...28..974A. doi:10.1364/OL.28.000974. PMID 12836750. .
- [58] Hitz, Breck (August 2003). "Origin of 'fiber fuse' is revealed" (<http://www.photonics.com/Article.aspx?AID=16745>). *Photonics Spectra*. . Retrieved 2011-01-23.
- [59] Seo, Koji; et al. (October 2003). "Evaluation of high-power endurance in optical fiber links" ([http://www.furukawa.co.jp/review/fr024/fr24\\_04.pdf](http://www.furukawa.co.jp/review/fr024/fr24_04.pdf)). *Furukawa Review* (24): 17–22. ISSN 1348-1797. . Retrieved 2008-07-05.
- [60] IEEE Spectrum: Electricity Over Glass (<http://spectrum.ieee.org/energy/the-smarter-grid/electricity-over-glass>). IEEE Spectrum. October 2005
- [61] Photovoltaic feat advances power over optical fiber – Electronic Products ([http://www2.electronicproducts.com/Photovoltaic\\_feat\\_advances\\_power\\_over\\_optical\\_fiber-article-olap01-jun2006-html.aspx](http://www2.electronicproducts.com/Photovoltaic_feat_advances_power_over_optical_fiber-article-olap01-jun2006-html.aspx)). 06/01/2006
- [62] Kouznetsov, D.; Moloney, J.V. (2003). "Highly efficient, high-gain, short-length, and power-scalable incoherent diode slab-pumped fiber amplifier/laser" ([http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?tp=&arnumber=1242365&isnumber=27838](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=1242365&isnumber=27838)). *IEEE Journal of Quantum Electronics* **39** (11): 1452–1461. Bibcode 2003JQE...39.1452K. doi:10.1109/JQE.2003.818311. .

## Further reading

- Gambling, W. A., "The Rise and Rise of Optical Fibers", *IEEE Journal on Selected Topics in Quantum Electronics*, Vol. 6, No. 6, pp. 1084–1093, Nov./Dec. 2000.
- Hecht, Jeff, *Understanding Fiber Optics*, 4th ed., Prentice-Hall, Upper Saddle River, NJ, USA 2002 (ISBN 0-13-027828-9).
- Mirabito, Michael M.A; and Morgenstern, Barbara L., *The New Communications Technologies: Applications, Policy, and Impact*, 5th. Edition. Focal Press, 2004. (ISBN 0-24-080586-0).
- Nagel S. R., MacChesney J. B., Walker K. L., "An Overview of the Modified Chemical Vapor Deposition (MCVD) Process and Performance", *IEEE Journal of Quantum Electronics*, Vol. QE-18, No. 4, p. 459, April 1982.
- Ramaswami, R., Sivarajan, K. N., *Optical Networks: A Practical Perspective*, Morgan Kaufmann Publishers, San Francisco, 1998 (ISBN 1-55860-445-6).
- VDV Works LLC *Lennie Lightwave's Guide To Fiber Optics*, <http://www.vdvworks.com/LennieLw/> © 2002-6.
- Friedman, Thomas L. (2007). *The World is Flat*. Picador. ISBN 978-0-312-42507-4. The book discusses how fiber optics has contributed to globalization, and has revolutionized communications, business, and even the distribution of capital among countries.
- GR-771, *Generic Requirements for Fiber Optic Splice Closures*, Telcordia Technologies, Issue 2, July 2008. (<http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?ID=SEARCH&DOCUMENT=GR-771&>) Discusses fiber optic splice closures and the associated hardware intended to restore the mechanical and environmental integrity of one or more fiber cables entering the enclosure.

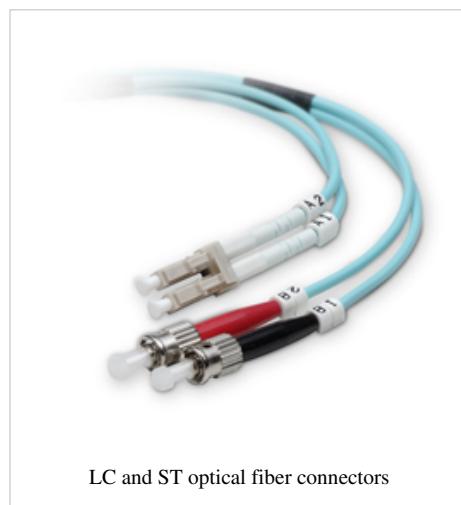
## External links

- The Fiber Optic Association (<http://www.thefoa.org/>)
- FOA color code for connectors (<http://www.thefoa.org/tech/connID.htm>)
- Lennie Lightwave's Guide To Fiber Optics (<http://www.jimhayes.com/lennielw/>)
- "Fibers (<http://www.rp-photonics.com/fibers.html>)", article in RP Photonics' *Encyclopedia of Laser Physics and Technology*
- How Fiber Optics are made (<http://www.fabilia.com/proyectos/ftth/tecnologia.asp>) In video
- "Fibre optic technologies ([http://www.gare.co.uk/technology\\_watch/fibre.htm](http://www.gare.co.uk/technology_watch/fibre.htm))", Mercury Communications Ltd, August 1992.

- " Photonics & the future of fibre ([http://www.gare.co.uk/technology\\_watch/photo.htm](http://www.gare.co.uk/technology_watch/photo.htm))", Mercury Communications Ltd, March 1993.
- " Fiber Optic Tutorial (<http://www.arcelect.com/fibercable.htm>)" Educational site from Arc Electronics
- " Plastic Optical Fiber (<https://sites.google.com/a/electronicbricks.it/electronicbricks/technologies-and-competitive-advantages/competitive-advantages-of-pof>)", Technologies and competitive advantages of POF – Plastic Optical Fiber
- MIT Video Lecture: Understanding Lasers and Fiberoptics (<http://ocw.mit.edu/resources/res-6-005-understanding-lasers-and-fiberoptics-spring-2008/laser-fundamentals-i/>)
- Fundamentals of Photonics: Module on Optical Waveguides and Fibers (<http://spie.org/Documents/Publications/00 STEP Module 07.pdf>)

## Optical fiber connector

An **optical fiber connector** terminates the end of an optical fiber, and enables quicker connection and disconnection than splicing. The connectors mechanically couple and align the cores of fibers so that light can pass. Better connectors lose very little light due to reflection or misalignment of the fibers.



LC and ST optical fiber connectors

### Application

Optical fiber connectors are used to join optical fibers where a connect/disconnect capability is required. The basic connector unit is a connector assembly. A connector assembly consists of an adapter and two connector plugs. Due to the polishing and tuning procedures that may be incorporated into optical connector manufacturing, connectors are generally assembled onto optical fiber in a supplier's manufacturing facility. However, the assembly and polishing operations involved can be performed in the field, for example, to make cross-connect jumpers to size.

Optical fiber connectors are used in telephone company central offices, at installations on customer premises, and in outside plant applications. Connectors are used to connect equipment and cables, or to cross-connect cables within a system.

Most optical fiber connectors are spring-loaded. The end faces of the fibers in the two connectors are pressed together, resulting in a direct glass to glass or plastic to plastic contact. This avoids a trapped layer of air between two fibers, which would increase connector insertion loss and reflection loss.

Every fiber connection has two values :

- Attenuation or insertion loss
- Reflection or return loss.

Measurements of these parameters are now defined in IEC standard 61753-1. The standard gives five grades for insertion loss from A (best) to D (worst), and M for multimode. The other parameter is return loss, with grades from 1 (best) to 5 (worst).

A variety of optical fiber connectors are available, but SC and LC connectors are the most common types of connectors on the market. Typical connectors are rated for 500–1,000 mating cycles.<sup>[1]</sup> The main differences among types of connectors are dimensions and methods of mechanical coupling. Generally, organizations will standardize on one kind of connector, depending on what equipment they commonly use. Different connectors are required for

multimode, and for single-mode fibers.

In datacom and telecom applications nowadays small connectors (e.g., LC) and multi-fiber connectors (e.g., MTP) are replacing the traditional connectors (e.g., SC), mainly to provide a higher number of fibers per unit of rack space.

Features of a good connector design:

- Low insertion loss
- High return loss (*low amounts of reflection at the interface*)
- Ease of installation
- Low cost
- Reliability
- Low environmental sensitivity
- Ease of use

Outside plant applications may involve locating connectors underground in subsurface enclosures that may be subject to flooding, on outdoor walls, or on utility poles. The closures that enclose them may be hermetic, or may be *free-breathing*. Hermetic closures will subject the connectors within to temperature swings but not to humidity variations unless they are breached. Free-breathing closures will subject them to temperature and humidity swings, and possibly to condensation and biological action from airborne bacteria, insects, etc. Connectors in the underground plant may be subjected to groundwater immersion if the closures containing them are breached or improperly assembled.

Depending on user requirements, housings for outside plant applications may be tested by the manufacturer under various environmental simulations, which could include physical shock and vibration, water spray, water immersion, dust, etc. to ensure the integrity of optical fiber connections and housing seals.

## Types

Many types of optical connector have been developed at different times, and for different purposes. Many of them are summarized in the table below.

**Fiber connector types**

Short name	Long form	Coupling type	Ferrule diameter	Standard	Typical applications
Avio (Avim)		Screw			Aerospace and avionics
ADT-UNI		Screw	2.5 mm		Measurement equipment
Biconic		Screw	2.5 mm		Obsolete
D4		Screw	2.0 mm		Telecom in the 1970s and 1980s, obsolete
Deutsch 1000		Screw			Telecom, obsolete
DIN (LSA)		Screw		IEC 61754-3	Telecom in Germany in 1990s; measurement equipment; obsolete
DMI		Clip	2.5 mm		Printed circuit boards
E-2000 (AKA LSH)		Snap, with light and dust-cap	2.5 mm	IEC 61754-15	Telecom, DWDM systems;
EC		push-pull type		IEC 1754-8	Telecom & CATV networks

ESCON	Enterprise Systems Connection	Snap (duplex)	2.5 mm		IBM mainframe computers and peripherals
F07			2.5 mm	Japanese Industrial Standard (JIS)	LAN, audio systems; for 200 µm fibers, simple field termination possible, mates with ST connectors
F-3000		Snap, with light and dust-cap	1.25 mm	IEC 61754-20	Fiber To The Home (LC Compatible)
FC	Ferrule Connector or <sup>[2]</sup> Fiber Channel	Screw	2.5 mm	IEC 61754-13	Datacom, telecom, measurement equipment, single-mode lasers; becoming less common
Fibergate		Snap, with dust-cap	1.25 mm		Backplane connector
FSMA		Screw	3.175 mm	IEC 60874-2	Datacom, telecom, test and measurement
LC	Lucent Connector <sup>[2]</sup> , Little Connector, or Local Connector	Snap	1.25 mm	IEC 61754-20	High-density connections, SFP transceivers, XFP transceivers
ELIO		Bayonet	2.5 mm	ABS1379	PC or UPC
Lucxis			1.25 mm	ARINC 801	PC or APC configurations (note 3)
LX-5		Snap, with light- and dust-cap		IEC 61754-23	High-density connections; rarely used
MIC	Media Interface Connector	Snap	2.5 mm		Fiber distributed data interface (FDDI)
MPO / MTP	Multiple-Fiber Push-On/Pull-off <sup>[2]</sup>	Snap (multiplex push-pull coupling)	2.5×6.4 mm <sup>[3]</sup>	IEC-61754-7; EIA/TIA-604-5 (FOCIS 5)	SM or MM multi-fiber ribbon. Same ferrule as MT, but more easily reconnectable. <sup>[3]</sup> Used for indoor cabling and device interconnections. MTP is a brand name for an improved connector, which intermates with MPO. <sup>[4]</sup>
MT	Mechanical Transfer	Snap (multiplex)	2.5×6.4 mm		Pre-terminated cable assemblies; outdoor applications <sup>[3]</sup>
MT-RJ	Mechanical Transfer Registered Jack or Media Termination - recommended jack <sup>[2]</sup>	Snap (duplex)	2.45×4.4 mm	IEC 61754-18	Duplex multimode connections
MU	Miniature unit <sup>[2]</sup>	Snap	1.25 mm	IEC 61754-6	Common in Japan
NEC D4		Screw	2.0 mm		Common in Japan telecom in 1980s
Opti-Jack		Snap (duplex)			
OPTIMATE		Screw			Plastic fiber, obsolete
OptoClip II		Snap (push-pull coupling)	None - bare fiber used	Proprietary Hüber & Suhner	Datacom and telecom; not common

SC	Subscriber Connector [2] or square connector [2] or Standard Connector	Snap (push-pull coupling)	2.5 mm	IEC 61754-4	Datacom and telcom; GBIC; extremely common
SMA 905	Sub Miniature A	Screw	Typ. 3.14 mm		Industrial lasers, military; telecom multimode
SMA 906	Sub Miniature A	Screw	Stepped; typ. 0.118 in ( <b>unknown operator: u'strong'</b> mm), then 0.089 in ( <b>unknown operator: u'strong'</b> mm)		Industrial lasers, military; telecom multimode
SMC	Sub Miniature C	Snap	2.5 mm		
ST / BFOC	Straight Tip [2]/Bayonet Fiber Optic Connector	Bayonet	2.5 mm	IEC 61754-2	Multimode, rarely single-mode; APC not possible (note 3)
TOSLINK	Toshiba Link	Snap		most common is JIS F05	Digital audio
VF-45		Snap			Datacom
1053 HDTV	Broadcast connector interface	Push-pull coupling	Industry-standard 1.25 mm diameter ceramic ferrule		Audio & Data (broadcasting)
V-PIN	V-System	Snap (Duplex) Push-pull coupling			Industrial and electric utility networking; multimode 200 µm, 400 µm, 1 mm, 2.2 mm fibers

## Notes

1. Modern connectors typically use a "physical contact" polish on the fiber and ferrule end. This is a slightly curved surface, so that when fibers are mated only the fiber cores touch, not the surrounding ferrules. Some manufacturers have several grades of polish quality, for example a regular FC connector may be designated "FC/PC" (for physical contact), while "FC/SPC" and "FC/UPC" may denote "super" and "ultra" polish qualities, respectively. Higher grades of polish give less insertion loss and lower back reflection.
2. Many connectors are available with the fiber end face polished at an angle to prevent light that reflects from the interface from traveling back up the fiber. Because of the angle, the reflected light does not stay in the fiber core but instead leaks out into the cladding. Angle-polished connectors should only be mated to other angle-polished connectors. Mating to a non-angle polished connector causes very high insertion loss. Generally angle-polished connectors have higher insertion loss than good quality straight physical contact ones. "Ultra" quality connectors may achieve comparable back reflection to an angled connector when connected, but an angled connection maintains low back reflection even when the output end of the fiber is disconnected.
3. Angle-polished connections are distinguished visibly by the use of a green strain relief boot, or a green connector body. The parts are typically identified by adding "/APC" (angled physical contact) to the name. For example, an angled FC connector may be designated FC/APC, or merely FCA. Non-angled versions may be denoted FC/PC or with specialized designations such as FC/UPC or FCU to denote an "ultra" quality polish on the fiber end face.
4. SMA 906 features a "step" in the ferrule, while SMA 905 uses a straight ferrule. SMA 905 is also available as a keyed connector, used e.g., for special spectrometer applications.

## Mnemonics

- LC connectors are sometimes called "Little Connectors".
- MT-RJ connectors look like a miniature 8P8C connector — commonly (but erroneously) referred to as RJ-45.<sup>[5][6]</sup>
- ST connectors refer to having a "straight tip", as the sides of the ceramic (which has a lower temperature coefficient of expansion than metal) tip are parallel—as opposed to the predecessor bi-conic connector which aligned as two nesting ice cream cones would. Other mnemonics include "Set and Twist", "Stab and Twist", and "Single Twist", referring to how it is inserted (the cable is pushed into the receiver, and the outer barrel is twisted to lock it into place). Also they are known as "Square Top" due to the flat end face.
- SC connectors have a mnemonic of "Square Connector", and some people believe that to be the correct name, rather than the more official "Subscriber Connector".<sup>[2]</sup> This refers to the fact the connectors themselves are square. Other terms often used for SC connectors are "Set and Click" or "Stab and Click".

## Images



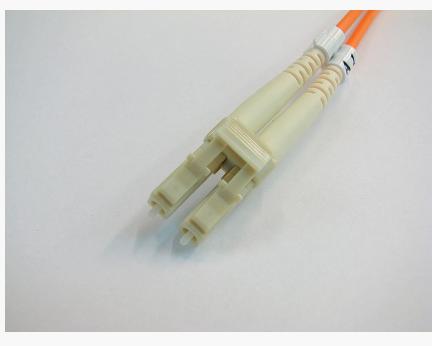
FC connector



E2000 connector



ESCON connector



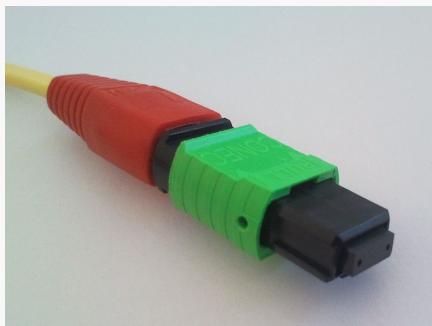
LC connector (duplex)



LuxCis connector



MIC (FDDI) connector



MPO connector



MT-RJ connector



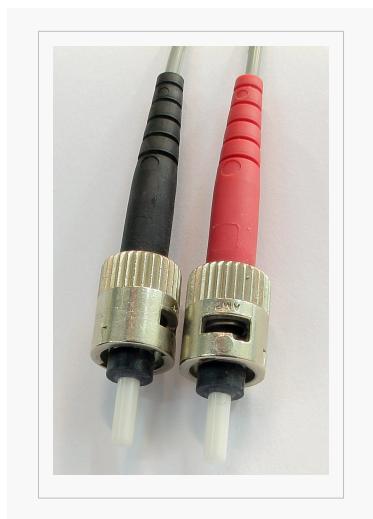
SC connector



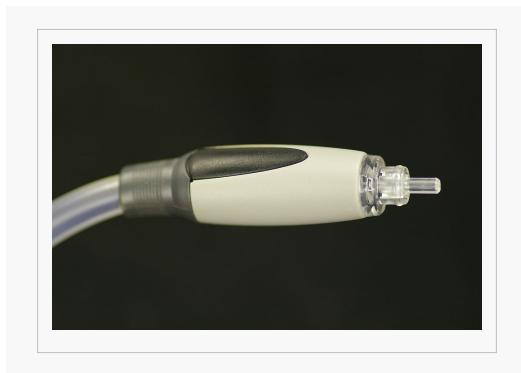
SC connector (duplex)



SMA 905 connectors



ST connector



TOSLINK connector

## Analysis

- *FC* connectors' floating ferrule provides good mechanical isolation. *FC* connectors need to be mated more carefully than the push-pull types due to the need to align the key, and due to the risk of scratching the fiber end face while inserting the ferrule into the jack. *FC* connectors have been replaced in many applications by *SC* and *LC* connectors.<sup>[7]</sup>
- There are two incompatible standards for key widths on *FC/APC* and polarization-maintaining *FC/PC* connectors: 2 mm ("Reduced" or "type R") and 2.14 mm ("NTT" or "type N").<sup>[8]</sup> Connectors and receptacles with different key widths either cannot be mated, or will not preserve the angle alignment between the fibers, which is especially important for polarization-maintaining fiber. Some manufacturers mark reduced keys with a single scribe mark on the key, and mark NTT connectors with a double scribe mark.
- *SC* connectors offer excellent packing density, and their push-pull design reduces the chance of fiber end face contact damage during connection; frequently found on the previous generation of corporate networking gear, using GBICs.
- *LC* connectors have replaced *SC* connectors in corporate networking environments due to their smaller size; they are often found on small form-factor pluggable transceivers.
- *ST* connectors have a key which prevents rotation of the ceramic ferrule, and a bayonet lock similar to a BNC shell. The single index tab must be properly aligned with a slot on the mating receptacle before insertion; then the bayonet interlock can be engaged, by pushing and twisting, locking at the end of travel which maintains spring-loaded engagement force on the core optical junction.
- In general the insertion loss should not exceed 0.75 dB and the return loss should be higher than 20 dB. Typical insertion repeatability, the difference in insertion loss between one plugging and another, is 0.2 dB.
- On all connectors, cleaning the ceramic ferrule before each connection helps prevent scratches and extends the connector life substantially.
- Connectors on polarization-maintaining fiber are sometimes marked with a blue strain relief boot or connector body, although this is far from a universal standard. Sometimes a blue buffer tube is used on the fiber instead.<sup>[9]</sup>
- *MT-RJ* (*Mechanical Transfer Registered Jack*) uses a form factor and latch similar to the 8P8C (*RJ45*) connectors. Two separate fibers are included in one unified connector. It is easier to terminate and install than *ST* or *SC* connectors. The smaller size allows twice the port density on a face plate than *ST* or *SC* connectors do. The *MT-RJ* connector was designed by AMP, but was later standardized as FOCIS 12 (Fiber Optic Connector Intermateability Standards) in EIA/TIA-604-12. There are two variations: pinned and no-pin. The pinned variety, which has two small stainless steel guide pins on the face of the connector, is used in patch panels to mate with the no-pin connectors on *MT-RJ* patch cords.

- *Hardened Fiber Optic Connectors (HFOCs) and Hardened Fiber Optic Adapters (HFOAs)* are passive telecommunications components used in an Outside Plant (OSP) environment. They provide drop connections to customers from fiber distribution networks. These components may be provided in pedestal closures, aerial and buried closures and terminals, or equipment located at customer premises such as a Fiber Distribution Hub (FDH) or an Optical Network Terminal or Termination (ONT) unit.

These connectors, which are field-mateable, and hardened for use in the OSP, are needed to support Fiber to the Premises (FTTP) deployment and service offerings. HFOCs are designed to withstand climatic conditions existing throughout the U.S., including rain, flooding, snow, sleet, high winds, and ice and sand storms. Ambient temperatures ranging from  $-40^{\circ}\text{C}$  ( $-40^{\circ}\text{F}$ ) to  $+70^{\circ}\text{C}$  ( $158^{\circ}\text{F}$ ) can be encountered.

Telcordia<sup>[10]</sup> contains the industry's most recent requirements for HFOCs and HFOAs.

## Testing

Glass fiber optic connector performance is affected both by the connector and by the glass fiber. Concentricity tolerances affect the fiber, fiber core, and connector body. The core optical index of refraction is also subject to variations. Stress in the polished fiber can cause excess return loss. The fiber can slide along its length in the connector. The shape of the connector tip may be incorrectly profiled during polishing. The connector manufacturer has little control over these factors, so in-service performance may well be below the manufacturer's specification.

Testing fiber optic connector assemblies falls into two general categories: factory testing and field testing.

Factory testing is sometimes statistical, for example, a process check. A profiling system may be used to ensure that the overall polished shape is correct, and a good quality optical microscope to check for blemishes. Optical Loss / Return Loss performance is checked using specific reference conditions, against a "reference standard" single mode test lead, or using an "Encircled Flux Compliant" source for multi-mode testing. Testing and rejection ("yield") may represent a significant part of the overall manufacturing cost.

Field testing is usually simpler. A special hand-held optical microscope is used to check for dirt or blemishes, and an optical time-domain reflectometer may be used to identify significant point losses or return losses. A power meter and light source or loss test set may also be used to check end-to-end loss.

## References

- [1] Alwayn, Vivek (2004). "Fiber-Optic Technologies" (<http://www.ciscopress.com/articles/article.asp?p=170740&seqNum=8>). . Retrieved Aug. 15, 2011.
- [2] Keiser, Gerd (August 2003). *Optical Communications Essentials*. McGraw-Hill Networking Professional. p. 132-. ISBN 0-07-141204-2.
- [3] Shimoji, Naoko; Yamakawa, Jun; Shiino, Masato (1999). "Development of Mini-MPO Connector" ([http://www.furukawa.co.jp/review/fr018/fr18\\_16.pdf](http://www.furukawa.co.jp/review/fr018/fr18_16.pdf)). *Furukawa Review* (18): 92..
- [4] "Frequently asked questions" (<http://www.usconec.com/pages/faq/faqfrm.html>). US Conec. . Retrieved 12 Feb 2009.
- [5] Trulove, James (December 19, 2005). "Designing LAN Wiring Systems". *LAN wiring* (3rd ed.). McGraw-Hill Professional. p. 23. ISBN 0-07-145975-8. "The 8-pin modular jack is sometimes referred to as an "RJ-45," because the connector/jack components are the same. However, RJ-45 actually applies to a special purpose jack configuration that is not used in LAN or standard telephone wiring."
- [6] Trulove, James (December 19, 2005). "Work Area Outlets". *LAN wiring* (3rd ed.). McGraw-Hill Professional. p. 132. ISBN 0-07-145975-8. "Modular jacks are often referred to as "RJ-45" jacks. This is not really the correct moniker, although it is in very common use."
- [7] Hayes, Jim (2005). "Connector Identifier" (<http://www.thefoa.org/tech/connID.htm>). *The Fiber Optic Association — Tech Topics*. . Retrieved Feb. 6, 2009.
- [8] Sezerman, Omur; Best, Garland (December 1997). "Accurate alignment preserves polarization" ([http://www.laserfocusworld.com/display\\_article/31401/12/none/none/News/Accurate-alignment-preserves-polarization](http://www.laserfocusworld.com/display_article/31401/12/none/none/News/Accurate-alignment-preserves-polarization)). *Laser Focus World*. . Retrieved March 12, 2009.
- [9] "Polarization maintaining fiber patchcords and connectors" ([http://www.ozoptics.com/ALLNEW\\_PDF/DTS0071.pdf](http://www.ozoptics.com/ALLNEW_PDF/DTS0071.pdf) (pdf)). *OZ Optics*. . Retrieved Feb. 6, 2009.
- [10] GR-3120, Issue 2, April 2010, Generic Requirements for Hardened Fiber Optic Connectors (HFOCs) and Hardened Fiber Optic Adapters (HFOAs) (<http://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?ID=SEARCH&DOCUMENT=GR-3120&>),
  - Fiber optic connectors ([http://www.fiber-optics.info/articles/fiber\\_optic\\_connectors](http://www.fiber-optics.info/articles/fiber_optic_connectors))
  - More fiber optic connectors (<http://www.fiberc.com>)

- Fiber optic connector identifier (<http://www.thefoa.org/tech/connID.htm>) (with pictures and more connectors)

## External links

- Fiber Optic Connector Reference ([http://www.ertyu.org/steven\\_nikkel/fiberconnect.html](http://www.ertyu.org/steven_nikkel/fiberconnect.html)) (with pictures)
- How To Terminate Fiber Optic Connectors - Pictures and Video (<http://discountlowvoltage.blogspot.com/2009/10/how-to-terminate-fiber-optic-cable.html>)
- Fiber optic connector termination processes (<http://www.vdvworks.com/VHO/fiberterm/index.html>)
- SC Connector termination anaerobic processes (<http://www.youtube.com/watch?v=kIYFLdlZ7a8>) (Video)

# Article Sources and Contributors

**Computer networking** *Source:* <http://en.wikipedia.org/w/index.php?oldid=427998888> *Contributors:* \*Kat\*, 10metreh, 149AFK, 16@r, 1966batfan, 28421u2232nfencenc, 28bytes, 2D, 5 albert square, 802geek, A520, ACBest, AJCham, ARUNKUMAR P.R, Ajaja, Abb615, Abraham, B.S., Acnetj, Adam1213, Adam850, Adambro, Addihockey10, AdjustShift, AeonicOmega, Aeonx, Aicchalmers, Aij, Aitias, Aj772, Akbpcb, Akendall, Alansohn, Aleenf1, AlexiusHoratius, Allens, Alpha 4615, Alphachimp, Altruism, Alucard 16, Amirrad.en, Amojobim, Anbu121, AndreasWittenstein, Andrew D White, Andrewcrawford, Andy16666, Aneah, Angrysockhop, Anna Lincoln, Anonauthor, Anonymi, Antandrus, Anupkeskar, Anurag trojan, Apau98, Apparition11, Apteva, Arctic Fox, ArglebargleIV, Armchair info guy, ArmenSokhakyan, Arthena, Atw1996, Avinash0147, Avoided, Avril0412, AzaToth, Banaticus, Baronnet, Bart133, Bassbonerocks, Beelaj, Bella Swan, Belovedfreak, BevinBrett, Bhasrini, Bhny, Bjankuloski06en, Black Falcon, Blanchard, Blaxthos, Blazerskj7315, BlueDevil, Blueraspberry, Bob f.it, Bobby122, Bobo192, Bokey97, Bokunenjin, Bongwarrior, Brandon, Brian Crawford, Btilm, BuddhaBubble, Bumpusjames, Bushsf, ButOnMethItIs, Bwmitchie, Bxn1358, C777, CBM, CWY2190, CWii, Cachiadavid, Caiaffa, Calltech, Caltas, Camw, Can You Prove That You're Human, Can't sleep, clown will eat me, CanadianLinuxUser, CapitalR, Capricorn42, Captain panda, Captain-tucker, Captainreiss, CardinalDan, Cbderdorset, Cerebellum, CesarB, Cgmusselman, Chad44, Chakkalokes, Chandlermbing, Chris the speller, Chrisch, Chriswiki, Chromaticity, Chzz, Clarince63, Closedmouth, Cnilep, Cnkids, Coeus559, CommonsDelinker, Corruptcopper, Courcelles, Cpiral, Cpl Syx, Cst17, Cstratacos, Cwils, Cwoodskareska, Cxz111, Cybercobra, Cyclonenim, D, D. Recorder, D.c.camero, DARTH SIDIOUS 2, DJBullfish, Dabomb87, Dac04, DakotaDAllen, DaltinWentsworth, DanMS, Daniel Procter, Danlaycock, Dap263, Darkkloud29, Darth Panda, Davosmith, Dayyanb, DeadEyeArrow, Decltype, Demonslayer4000, Denisarona, DerHexer, Dgtsyb, Dgw, Diannaa, Dicklyon, Dipankar001, Discospinster, Djg2006, Djmckee1, Dlohcierkeim, Dotancohen, DoubleBlue, Download, Dreadstar, Dwayne, DyingIce, Dylan620, EarthPerson, Easwarno1, Edward, Eekster, Egggnogicecream, Egmontaz, Eitheladar, Eleos, Elinruby, Elphion, Emailtonaved, EncMstr, Enigmaman, Ephr123, Er Komandante, Eraxx, Erdog'an said, Erianna, Eric-Wester, Escape Orbit, EvokeNZ, Excirial, Extransit, FJPB, Face, Faithlessthewonderboy, Falcon8765, Faradayplank, Favonian, FaysallF, Fazlurrahman95, Fgrose, Fieldday-sunday, Fifwekid, Figma, Finnysgay, Fintanmurphy, Fireaxe888, Fireice, Firien, Flewis, Flyingcheese, Fozz79, Frankie0607, Freedominux, Frmatt, Funnyfarmdoofmo, Fyfer, Fae, GLaDOS, GNMC, Gail, GandalfDaGraay, Ghola, Giftlite, Glane23, Glenn, Gnowor, Gogo Dodo, GoingBatty, Gonchibolso12, GoneAwayNowAndRetired, Grafen, Greennd, GroveGuy, Guggfe, Gurch, Gurchzilla, Gv250, Gyan pokhara, Hammersoft, Happyssailor, HarisM, Harryzilber, Harshateria, Haseo9999, Heberkowitz, Hchrn, Headbom, Hellkitylover12, Hemachandra18, Herbythyme, HDrNick, Hpcanswers, Hut 8.5, INKubus, Iammillner, Igoldste, Imroy, Incompetence, Indon, Inseesiyou, Intgr, Ipatrol, Iridescent, IronGargoyle, It4it-wiki, Itus15q4user, J. Martin Wills, J.delanoy, JBazuzi, JEBrown87544, JLRedperson, JLaTondre, Jackelfive, Jackfork, Jackol, Jake Wartenberg, Jan1nad, Japheth the Warlock, Jared Preston, Jasper Deng, Jauerback, Jay, Jayakrishnan0804, Jclemons, Jeepday, Jeff G., Jer71, Jerzy, Jlabourdette, Jheyahr, Jimmi Hugh, Jjsi, Jjensen347, Jjron, Jni, Joantorres, Joelhanley, John Stumbles, Johnuniq, JonHarder, Jordanfeldman, Joseph Solis in Australia, Joshua Gyamfi, Joshua Scott, Joy, Jpbown, Jprg1966, Jxl180, KGasso, Kazochi, Kbrose, Keilana, KelleyCook, Kgflieschmann, Kieferb12, King of Hearts, Kingpin13, Kms, KnowBuddy, Knowz, Koffieyaho, Koolabsol, Kozuch, Kranix, Krishnaveda, Krj373, Kudret abi, Kushalwas777, Kvng, L Kensington, L314t, L33th4x0rguy, LFaraone, Landon1980, Leafyplant, LeaveSleaves, LeinaD natipac, Levineps, Leye1, Lightmouse, Lights, Lilac Soul, Lillightning, Limideen, LindsayH, Ling.Nut, Loile0801, Lotje, Lucky arien2001, Ludovic, ferre, Luk, Lukeritiche, MER-C, Macbookmiller, Macy, Madcoverboy, Madhero88, Magioladitis, Maismuhanad, Mandarax, Maneendra, Manjax76, Marco94, Marek69, Mark Arsten, Mark91, MarkBolton, Markdu09, MarkmacVSS, Mascharanas, Masterjamie, Matdrodes, Mattgirling, Mattl2001, McSly, Mdd, MelbourneStar, Mentifisto, Mephistophelian, Metropicopolis, Michael Angelkovich, Michael93555, Micke-sv, Mikae, Mike Rosoft, Mike.lifeguard, MikhailVS, Milind m2255, Mindmatrix, Minimac, Minimac's Clone, Misiorite, MisterCharlie, Miym, Mlewiso00, Mlouns, Mmernex, Mmmeg, Modamoda, Monchav, Montrevux, MorrisRob, Mottsauce, Mr. Wheely Guy, MrSmook, MrNatural, MuZemike, Muhandes, My76Strat, Mynameiswill, N5iln, NYKevin, Nanzilla, Nathani, NawlinWiki, Nazi 2007, Neillucas, NeoJustin, Nepenthess, Netalarm, Nethgir, Netito777, Networkingguy, NewEnglandYankee, Ngriffeth, Nihilites, Nopetro, Northamerica1000, NorwegianBlue, NoticeBored, Novalis, Nrm123, Nsda, Nubiotech, Nurg, Nurlan926, Ojasweesharma, Oliver202, OllieFury, Onure, Opelio, Orange Suede Sofa, Orbst, Oros, Otolemur crassicaudatus, OverlordQ, Oxymoron83, PAntoni, Padillah, Pakakj.20june, Pascal.Tesson, PatrikR, Paul August, Pchov, Pdcook, Pedro, Peterwhy, PhJ, Pharaoh of the Wizards, Phatom87, PhilKnight, Philip Trueman, PhilipJS, Phoe6, Piano non troppo, Pigman, Pill, Pinethicket, Pingveno, Plaga701, PleaseStand, Polluxian, Porkind, Porterjoh, Possum, Poweroid, Prari, Prashanthns, Promethean, Public Menace, Puffin, Pwarrior, Pxma, Pyrospirit, Quaeler, Quantpole, Qwyrian, Qxz, R'n'B, RJaguar3, RadioFan, Radon210, Raed abu farha, Rahul440, RainbowOfLight, Rananera74, Rangek, Rangoon11, Raven21421, Razaraipoot, Razertek, Rctay, Reaper Eternal, Red Thrush, Reliableforever, Rememberway, Renewer, Rettetast, Riana, Ricardoprojects, Rick Block, Riick, Rjd0060, Rmaheshnaidu, Rmosler2100, RoMo37, Robertllston, Roland Kaufmann, Rpsjrepa, Rsrikanth05, Rwww, Ryan Vesey, RyanCross, Ryulong, SMC, ST47, Saketmitra, Sandeepsp4u, Satori Son, Sayedomer, Segtrp, SchreiberBike, Sciruriae, Scottywong, Seaphoto, Seek54, Sephiroth BCR, Sesu Prime, Sgeo, Shadowjams, Shanes, Shemne, Shiawakant.bharti, ShornAssociates, Sigma 7, Skarebo, Skizzik, SkyWalker, Skyzeey, Slawekb, Slon02, SmartGuy Old, Smokizzy, SoCalSuperEagle, Soap Poisoning, Some jerk on the Internet, Sonjaaa, SpaceFlight89, SpecMode, Special Cases, Spitfire, Spmeyn, SpuriousQ, Ssmorris, StaleOnion, SteinbDJ, Stephan Leeds, Stephenb, SteveO, Storm Rider, Strike Eagle, Stwalkerster, SudoGhost, Suffusion of Yellow, Sumitprksh, SuperSlacker, Symetrix, Synchronism, Syrthiss, Tango, Tarif Ezaz, Tbhottch, Teapeat, TechTWI, Technobadger, Terrek, Testbells, Tgeairn, The Thing That Should Not Be, TheCatalyst31, Wknigh94, Wolfkeeper, Woohookitty, Wtmitchell, Wtsao, Wuhwuzdat, Xompanthy, YassineMrabet, Zawthet, Zedex7, Zentraleinheite, Zzuuzz, مجموعه عالم, شات صوتي, ترجمان, طبع - ج ٢٠١٥, ٢٨٧١ anonymous edits

**Computer network** *Source:* <http://en.wikipedia.org/w/index.php?oldid=509740195> *Contributors:* \*Kat\*, 10metreh, 149AFK, 16@r, 1966batfan, 28421u2232nfencenc, 28bytes, 2D, 5 albert square, 802geek, A520, ACBest, AJCham, ARUNKUMAR P.R, Ajaja, Abb615, Abraham, B.S., Acnetj, Adam1213, Adam850, Adambro, Addihockey10, AdjustShift, AeonicOmega, Aeonx, Aicchalmers, Aij, Aitias, Aj772, Akbpcb, Akendall, Alansohn, Aleenf1, AlexiusHoratius, Allens, Alpha 4615, Alphachimp, Altruism, Alucard 16, Amirrad.en, Amojobim, Anbu121, AndreasWittenstein, Andrew D White, Andrewcrawford, Andy16666, Aneah, Angrysockhop, Anna Lincoln, Anonauthor, Anonymi, Antandrus, Anupkeskar, Anurag trojan, Apau98, Apparition11, Apteva, Arctic Fox, ArglebargleIV, Armchair info guy, ArmenSokhakyan, Arthena, Atw1996, Avinash0147, Avoided, Avril0412, AzaToth, Banaticus, Baronnet, Bart133, Bassbonerocks, Beelaj, Bella Swan, Belovedfreak, BevinBrett, Bhasrini, Bhny, Bjankuloski06en, Black Falcon, Blanchard, Blaxthos, Blazerskj7315, BlueDevil, Blueraspberry, Bob f.it, Bobby122, Bobo192, Bokey97, Bokunenjin, Bongwarrior, Brandon, Brian Crawford, Btilm, BuddhaBubble, Bumpusjames, Bushsf, ButOnMethItIs, Bwmitchie, Bxn1358, C777, CBM, CWY2190, CWii, Cachiadavid, Caiaffa, Calltech, Caltas, Camw, Can You Prove That You're Human, Can't sleep, clown will eat me, CanadianLinuxUser, CapitalR, Capricorn42, Captain panda, Captain-tucker, Captainreiss, CardinalDan, Cbderdorset, Cerebellum, CesarB, Cgmusselman, Chad44, Chakkalokes, Chandlermbing, Chris the speller, Chrisch, Chriswiki, Chromaticity, Chzz, Clarince63, Closedmouth, Cnilep, Cnkids, Coeus559, CommonsDelinker, Corruptcopper, Courcelles, Cpiral, Cpl Syx, Cst17, Cstratacos, Cwils, Cwoodskareska, Cxz111, Cybercobra, Cyclonenim, D, D. Recorder, D.c.camero, DARTH SIDIOUS 2, DJBullfish, Dabomb87, Dac04, DakotaDAllen, DaltinWentsworth, DanMS, Daniel Procter, Danlaycock, Dap263, Darkkloud29, Darth Panda, Davosmith, Dayyanb, DeadEyeArrow, Decltype, Demonslayer4000, Denisarona, DerHexer, Dgtsyb, Dgw, Diannaa, Dicklyon, Dipankar001, Discospinster, Djg2006, Djmckee1, Dlohcierkeim, Dotancohen, DoubleBlue, Download, Dreadstar, Dwayne, DyingIce, Dylan620, EarthPerson, Easwarno1, Edward, Eekster, Egggnogicecream, Egmontaz, Eitheladar, Eleos, Elinruby, Elphion, Emailtonaved, EncMstr, Enigmaman, Ephr123, Er Komandante, Eraxx, Erdog'an said, Erianna, Eric-Wester, Escape Orbit, EvokeNZ, Excirial, Extransit, FJPB, Face, Faithlessthewonderboy, Falcon8765, Faradayplank, Favonian, FaysallF, Fazlurrahman95, Fgrose, Fieldday-sunday, Fifwekid, Figma, Finnysgay, Fintanmurphy, Fireaxe888, Fireice, Firien, Flewis, Flyingcheese, Fozz79, Frankie0607, Freedominux, Frmatt, Funnyfarmdoofmo, Fyfer, Fae, GLaDOS, GNMC, Gail, GandalfDaGraay, Ghola, Giftlite, Glane23, Glenn, Gnowor, Gogo Dodo, GoingBatty, Gonchibolso12, GoneAwayNowAndRetired, Grafen, Greennd, GroveGuy, Guggfe, Gurch, Gurchzilla, Gv250, Gyan pokhara, Hammersoft, Happyssailor, HarisM, Harryzilber, Harshateria, Haseo9999, Heberkowitz, Hchrn, Headbom, Hellkitylover12, Hemachandra18, Herbythyme, HDrNick, Hpcanswers, Hut 8.5, INKubus, Iammillner, Igoldste, Imroy, Incompetence, Indon, Inseesiyou, Intgr, Ipatrol, Iridescent, IronGargoyle, It4it-wiki, Itus15q4user, J. Martin Wills, J.delanoy, JBazuzi, JEBrown87544, JLRedperson, JLaTondre, Jackelfive, Jackfork, Jackol, Jake Wartenberg, Jan1nad, Japheth the Warlock, Jared Preston, Jasper Deng, Jauerback, Jay, Jayakrishnan0804, Jclemons, Jeepday, Jeff G., Jer71, Jerzy, Jlabourdette, Jheyahr, Jimmi Hugh, Jjsi, Jjensen347, Jjron, Jni, Joantorres, Joelhanley, John Stumbles, Johnuniq, JonHarder, Jordanfeldman, Joseph Solis in Australia, Joshua Gyamfi, Joshua Scott, Joy, Jpbown, Jprg1966, Jxl180, KGasso, Kazochi, Kbrose, Keilana, KelleyCook, Kgflieschmann, Kieferb12, King of Hearts, Kingpin13, Kms, KnowBuddy, Knowz, Koffieyaho, Koolabsol, Kozuch, Kranix, Krishnaveda, Krj373, Kudret abi, Kushalwas777, Kvng, L Kensington, L314t, L33th4x0rguy, LFaraone, Landon1980, Leafyplant, LeaveSleaves, LeinaD natipac, Levineps, Leye1, Lightmouse, Lights, Lilac Soul, Lillightning, Limideen, LindsayH, Ling.Nut, Loile0801, Lotje, Lucky arien2001, Ludovic, ferre, Luk, Lukeritiche, MER-C, Macbookmiller, Macy, Madcoverboy, Madhero88, Magioladitis, Maismuhanad, Mandarax, Maneendra, Manjax76, Marco94, Marek69, Mark Arsten, Mark91, MarkBolton, Markdu09, MarkmacVSS, Mascharanas, Masterjamie, Matdrodes, Mattgirling, Mattl2001, McSly, Mdd, MelbourneStar, Mentifisto, Mephistophelian, Metropicopolis, Michael Angelkovich, Michael93555, Micke-sv, Mikae, Mike Rosoft, Mike.lifeguard, MikhailVS, Milind m2255, Mindmatrix, Minimac, Minimac's Clone, Misiorite, MisterCharlie, Miym, Mlewiso00, Mlouns, Mmernex, Mmmeg, Modamoda, Monchav, Montrevux, MorrisRob, Mottsauce, Mr. Wheely Guy, MrSmook, MrNatural, MuZemike, Muhandes, My76Strat, Mynameiswill, N5iln, NYKevin, Nanzilla, Nathani, NawlinWiki, Nazi 2007, Neillucas, NeoJustin, Nepenthess, Netalarm, Nethgir, Netito777, Networkingguy, NewEnglandYankee, Ngriffeth, Nihilites, Nopetro, Northamerica1000, NorwegianBlue, NoticeBored, Novalis, Nrm123, Nsda, Nubiotech, Nurg, Nurlan926, Ojasweesharma, Oliver202, OllieFury, Onure, Opelio, Orange Suede Sofa, Orbst, Oros, Otolemur crassicaudatus, OverlordQ, Oxymoron83, PAntoni, Padillah, Pakakj.20june, Pascal.Tesson, PatrikR, Paul August, Pchov, Pdcook, Pedro, Peterwhy, PhJ, Pharaoh of the Wizards, Phatom87, PhilKnight, Philip Trueman, PhilipJS, Phoe6, Piano non troppo, Pigman, Pill, Pinethicket, Pingveno, Plaga701, PleaseStand, Polluxian, Porkind, Porterjoh, Possum, Poweroid, Prari, Prashanthns, Promethean, Public Menace, Puffin, Pwarrior, Pxma, Pyrospirit, Quaeler, Quantpole, Qwyrian, Qxz, R'n'B, RJaguar3, RadioFan, Radon210, Raed abu farha, Rahul440, RainbowOfLight, Rananera74, Rangek, Rangoon11, Raven21421, Razaraipoot, Razertek, Rctay, Reaper Eternal, Red Thrush, Reliableforever, Rememberway, Renewer, Rettetast, Riana, Ricardoprojects, Rick Block, Riick, Rjd0060, Rmaheshnaidu, Rmosler2100, RoMo37, Robertllston, Roland Kaufmann, Rpsjrepa, Rsrikanth05, Rwww, Ryan Vesey, RyanCross, Ryulong, SMC, ST47, Saketmitra, Sandeepsp4u, Satori Son, Sayedomer, Segtrp, SchreiberBike, Sciruriae, Scottywong, Seaphoto, Seek54, Sephiroth BCR, Sesu Prime, Sgeo, Shadowjams, Shanes, Shemne, Shiawakant.bharti, ShornAssociates, Sigma 7, Skarebo, Skizzik, SkyWalker, Skyzeey, Slawekb, Slon02, SmartGuy Old, Smokizzy, SoCalSuperEagle, Soap Poisoning, Some jerk on the Internet, Sonjaaa, SpaceFlight89, SpecMode, Special Cases, Spitfire, Spmeyn, SpuriousQ, Ssmorris, StaleOnion, SteinbDJ, Stephan Leeds, Stephenb, SteveO, Storm Rider, Strike Eagle, Stwalkerster, SudoGhost, Suffusion of Yellow, Sumitprksh, SuperSlacker, Symetrix, Synchronism, Syrthiss, Tango, Tarif Ezaz, Tbhottch, Teapeat, TechTWI, Technobadger, Terrek, Testbells, Tgeairn, The Thing That Should Not Be, TheCatalyst31, Wknigh94, Wolfkeeper, Woohookitty, Wtmitchell, Wtsao, Wuhwuzdat, Xompanthy, YassineMrabet, Zawthet, Zedex7, Zentraleinheite, Zzuuzz, مجموعه عالم, شات صوتي, ترجمان, طبع - ج ٢٠١٥, ٢٨٧١ anonymous edits

Thejatclubrock, Thejokerface, Theopolisme, Thetaung, Think outside the box, Thrindel, Thumperward, Tiddly Tom, Tide rolls, Titoxd, Todd Peng, Tombomp, Tony1, Topbanana, Toussaint, Traxs7, Trenwith, TreveX, Trgaz, Triona, Triwbe, Tropyor, Tslocum, Turabsf, Turgan, TutterMouse, TyA, Tyrol5, UBJ 43X, UU, Ulric1313, Ultimarko, Uncle Dick, UncleDougie, Vamphemu, VandalCruncher, Vanished user 39948282, Vanka5, Versageek, Versus22, VictorAnyakin, Visaforu, Visor, VooDooChild, Vrenator, W Nowicki, Wa3frp, Wadamja, Walter.bender, Waryklingon, Watchdog9, Wbm1058, Weezey, Welsh, Whereizben, WhisperToMe, WikHead, Wikipelli, Wikipixel, Wilde Jagd, Wimt, Wine Guy, Winston Chuen-Shih Yang, Wizardist, Wknigh94, Wolfkeeper, Woohookitty, Wtmitchell, Wtsao, Wuuhuzdat, Xompanthy, YassineMrabet, Zawthet, Zedex7, Zentraleinheite, Zzuuzz, محبوب عالم, شات صوتي, ٥٥, مجنون, טבינה-ה- 2871 anonymous edits

**Local area network** Source: <http://en.wikipedia.org/w/index.php?oldid=509490323> Contributors: 13magilj, 16@r, Ijohnny 1269, 2mcm, A beast with claws, Aapo Laitinen, Abarry, Abresas, Academic Challenger, Activ Banana, Affray, Ahoerstemeier, Aka, Akhilsharma86, Alansohn, Aldie, Aleksanda Bulovic', Alexandria, Alfio, AlisonW, AlistairMcMillan, Amaraiel, Ameliator!, Aneah, Angela, Anguskywong, Animum, Anrie Nord, Antandrus, Arjun01, ArmondoSC, Arthena, Astral9, Athenaara, Atlant, AxelBoldt, Bagatelle, Barry26, Beland, Ben-Zin, Bingo-101a, Biot, Bobblewik, Bongwarrior, Born2cycle, Bovineone, Brianga, BrokenSsegue, Brovnik, Brt100, Bryan Derksen, Bthebest, C0N6R355, CONF1Q, Camw, Can't sleep, clown will eat me, Canderison7, CapitalR, Catmoongirl, Ceros, CharlieGalik, Chic075, Chris jones the man, Chris the speller, Chriswiki, Chuq, Cipher text, Citcat, Ckatz, Closeapple, Closedmouth, Cmichael, Colorprobe, Commander, Commander Keane, CommonsDeligner, Comrade009, Conversion script, Coolmaxi898, Cpl Syx, Cst17, Cy0x, Cybercobra, DARTH SIDIOUS 2, DStoykov, Danelo, Darkeffekt, Darkmaster2004, Darth Panda, Dave Farquhar, Daverocks, DavidCary, Davismargaret, Dawd, Dawnseeker2000, Daz 90, Dead3y3, DeadEyeArrow, Delirium, Delldot, Demize, DerHexer, Dgtsy, Discospinster, DonConquistador, Dotancohen, Driftkid92, Eeekster, Emijrp, Enviroboy, Ebpr123, Escape Orbit, Evice, Excirial, Exer 505, Exir Kamalabadi, Exposit, Fagiolonero, Falcon8765, Farchand, Feydey, FiP, Frankenpuppy, Frap, Frecklefoot, Fullerene, Fæ, Gail, Gaius Cornelius, Gareth Griffith-Jones, Gcorbaz, Gertjanmeteenboomstam, Giftlite, Gilliam, Glenn, Grafen, Grey Shadow, Gsmgn, Hadal, Haffner, Hall Monitor, Hannes Hirzel, Haon, HarisM, Harryzilber, Hbk cmd, Headbomb, Hennessey, Patrick, Herr Beethoven, HIDrNick, Hmains, Hope(N Forever), Hovea, Husond, I feel Tired, Iammillner, Ibc111, Ice Cold Beer, Ilario, Immunine, InvertRect, Iricigor, IrisKawling, Irishguy, IronGargoyle, Itusg15q4user, J wood hail, J. M., J.delanoy, JLaTondre, JRamlow, Jackfork, JamesBWatson, Jason Patton, Jcw69, JediLofty, Jjensen347, JoeDaStood, Joebediah, Johnunq, JonHarder, Jondel, Joowww, Jorunn, Juliancolton, Jvano, Jóna Pórunn, KGasso, Karanne, Katieh5584, Kbrose, Kcufuoyokifyounowhtim, KelleyCook, KennethJ, KennyRogerz, Kingpin13, KnowledgeOfSelf, Koki.s, Kondody, Kushalbiswas777, Kvng, L Kensington, LarryQ, Lcsrms, Lemcmaster, Libcup, Lifartan, London2012, Lonewolf BC, Lorany21k, Lradrama, Luna Santin, Lupin, MIT Trekkie, MTurpin, MaestroX, Mahjongg, Mandarax, Manop, Marshall Williams2, Mashby, Materialscientist, Mathonius, Matthäus Wander, Mayur, Mbbs, Mdanhan2002, MerlinYoda, MessiFCB, Metricopolus, Micky140391, Mild Bill Hiccup, Mindmatrix, Mpjpieters, Mogulu, MonkeyFox, Monkeyman, Monopolyisgreat, Mortein, Mozillar, Mr Bound, Mtking, Myri fan, Mzub, NNU-1-05100211, Naniwako, Nanshu, Neon white, Networkingguy, Nmacu, Norm, Northamerica1000, Nubiatech, Ocee, Ohnoitsjamie, Ohyassie, Onorem, Ossworks, Owchowch, Oxymoron83, PL290, Panoramix, Patrick, Patstuart, Pcb21, Pdicario1986, Perfecto, Peter McGinley, PetersSymonds, Peyre, Phantomsteve, Phatom87, PhilipMW, Philomathoholic, Pierre-Yves Schütz, Pigsonthewing, Pill, Pjoe, Plugwash, Pmj, Polly, Povtula, Poweroid, Prashanthns, PrestonH, PseudoSudo, Psychonaut, Quaque, Quester, Quibik, Qx132, Qzwxeccexwzq, REP93, Rajubanka, Raven4x4x, Rawrxmimi, Reach Out to the Truth, Reconsider the static, Rees11, Requestion, Rgoondermote, Rick Sidwell, Ricsi, Rjstotl, Robertviews, Rocastole, Roy Baty, Rsm9833, SD5, Sam Hocevar, SanGatiche, Samse, Savio mit electronics, ScottSteiner, Sdowg, Seaphoot, Shanes, Sitethief, SixSix, Skapur, Skittleys, Skor, SkyWalker, Slipmikeknob, Smilesfozwood, Snafflekid, Snori, Snyses, Solipsist, Soosed, Spliffy, SpuriousQ, Stdazi, Stefan h, Stephen, Stuart Morrow, StubbyT, SurreyGaming, Sylvanwulf, Syncategoremeta, THEN WHO WAS PHONE?, Taelus, Teles, The Adventurer, The Anome, The Thing That Should Not Be, TheKMan, Thejerm, Thelesapandwack, Thumperward, Tide rolls, Tiger xox, Tkynerd, Tony6ty4ur, Tregoweth, Tripodics, Trollingftw, Troy 07, Trusilver, Tslocum, Turlo Lomon, Ulric1313, Urgos, Vaidyanathanparli, VampWillow, Villarinho, Violetriga, Vipinhar, Vybr8, Wadamja, Waggers, Wavelength, Wayward, Wernher, Wertoose, Weylinp, WikHead, Wikicraizer2011, Wikieditor06, Wikilibrarian, Wikipelli, Willy on Wheels over Ethernet, Windowsvistafan, Wipe, Wizardist, Woohookitty, Witt, Xaldafax, Yair rand, Yamamoto Ichiro, Yudiweb, Zachlipton, ZooFari, Zundark, Zzuuzz, İnanmu, 906 anonymous edits

**Campus area network** Source: <http://en.wikipedia.org/w/index.php?oldid=503909378> Contributors: Aapo Laitinen, Alexandria, Ali Esfandiari, Axl, Chris G, ChrisGualtieri, Cordless Larry, Cybercobra, English06, Erianna, Hadal, Hodg, JonHarder, Kbdank71, Kbrose, Kocio, Kvng, Ludovic.ferre, MendedAxe, Nat682, NigelJ, Nwatson, Oxymoron83, Panarchy, Rkononenko, Saaga, Suruena, Thief12, Thingg, UNHchabo, Utcursh, Vikiçizer, Viriditas, W Nowicki, Willemo, Woohookitty, 42 anonymous edits

**Metropolitan area network** Source: <http://en.wikipedia.org/w/index.php?oldid=496137114> Contributors: ABF, Acroterion, Aldie, Andrewwjensen, Anguskywong, Asubed2, Avono, Bensaccout, Blake-, Bleifu, Bobblewik, Borgx, CBOrgatope, Caltas, Carbuncle, Cesarc, Cmdrjameson, Cob, Cocytus, ConCompS, Cy0x, Cybercobra, Duffman, Ebpr123, Excirial, Flowerpower16, Fregle, Gareth Griffith-Jones, Gf up, Gulsumyilmaz, Hadal, Hallmark, HarisM, Hgferman, Hike395, Human step, Hydrogen Iodide, Ilario, Itai, Jake Wartenberg, Jdstroy, JonHarder, KGasso, KANE5187, Kbdank71, Kbrose, Keilana, Koem, Kozuch, Lemontea, Lifartan, Lollergay, LongHairedRedeck, M412k, Maher2777, Manop, Mark1800, Materialscientist, Namik, Nsjapan, Omegatron, Patrick, Phjellming, Quar, Raanoo, Radiosband, Rich Farmbrough, Rkononenko, Ryans, Sadrettin, Sam Korn, Sean01, Silvestre Zabala, SlowByte, SpeedyGonsales, Stephen Gilbert, StephenBuxton, Suradnik13, ThaddeusB, The Anome, The Thing That Should Not Be, TheRanger, Thinggg, Tom Morris, UNHchabo, VampWillow, Vegaswikian1, Violetriga, Viriditas, Will Beback, Xezbeth, Ykhwong, Zigger, Тверополник, 168 anonymous edits

**Wide area network** Source: <http://en.wikipedia.org/w/index.php?oldid=505739984> Contributors: A5b, ADVENT Gray, Aapo Laitinen, Adolphus79, Ageekgal, Ahoerstemeier, Aldie, Allstarecho, Amirrad, Anetode, Anodynus, Anomie, Apau98, Bakester69, Betacommmand, Big Smooth, Bishome, Bluezy, Bobblewik, Bobo192, Boing! said Zebedee, Brhoden, Brovnik, Can't sleep, clown will eat me, Cdboi, Chasingsol, Click23, ClickRick, Closedmouth, Colonies Chris, Cometstyles, Cpl Syx, Craven08, Cwinthe360, Cybercobra, DFS454, DVdn, Dascorpion88, Dead3y3, Deathtrap3000, Denisaron, Dgtsy, Dgw, Diberri, Djig2006, Doczilla, Doulos Christos, DudleyDoWrite, Duttler, Earlylpsychosis, Edward, Eeekster, Elkman, Ebpr123, Espoo, Frostie, Fss123, Funvill, Fvw, Gary Kirk, Gilliam, GlassCobra, Glenn, Greenmage801, Gzkn, Hadal, Harej, HarisM, Harryzilber, Hasek is the best, Hashar, Hu12, Ilario, IronGargoyle, J.delanoy, JamesMS, Japo, JayC, Jeffrey Sharkey, Jessejohnston, Job614, Joe King, John Riemann Soong, JonHarder, Juanpd, Juliancolton, Jóna Pórunn, Kbdank71, Kbrose, Keithonearth, Kingpin13, Kjkolb, Kungfuadam, Kvng, Kweku, Labklare, LeeJames, LiDaobing, LibLord, Lifartan, Lightmouse, Loftenter, Ltaylor, MER-C, MK8, Manop, Marko951, May, Mbimmler, Mcclurg, Mel Etitis, Minos the judge, Miquonranger03, Miteshspatel2, Mlewiss000, MrNerdHarr, Mulad, Naveen.maurya, NawlinWiki, Ndenson, Nick Ottery, Nick125, Norm, Northamerica1000, Northgrove, O.Koslowski, Odiumjunkie, OlEnglish, Onceler, One-t, Opelio, Optichan, Phatom87, PhilipO, Porkrind, Povtula, Prashanthns, Quinsareth, Raghith, Ratiocinate, Rcooley, Reach Out to the Truth, Reggane.M, Rhobite, Rich Farmbrough, Rjm at sleepers, Royb95, Ruggo, Ryan Postlethwaite, SEVEREN, Saibod, Schneeclocke, Shafqatz, Shriram, Shupzv3, Simon naylor, SimonP, Sirjective, SivaKumar, Skor, Snigbrook, Snowful, Soundray, Springnut, Syncategoremeta, Synchronism, Telavel, Techman224, TestPilot, The Stoneman, The andyman 0, TheClownDawg, Theo10011, Theresa knott, Tide rolls, Todd Vierling, Topsadow, Trusilver, Turbochr, Urgos, VampWillow, Vanished user 90345uijf983j4tc234k, Versageek, Viriditas, W Nowicki, Wa3frp, Wayne Slam, Wayward, WhyBeNormal, WikHead, Wikiborg, Wikicraizer2011, Wikipelli, Wilmt, Woohookitty, Wrs1864, Yst, Yudiweb, Zachlipton, Zfr, ПІс-прирзар, 433 anonymous edits

**Wi-Fi Hotspot** Source: <http://en.wikipedia.org/w/index.php?oldid=507088133> Contributors: A314268, Adamamu, Adrianjcunliffe, Aeonsafe, Airspot, Alangdon86, Alanrivazgonzalez, Alansohn, AlexHe34, AlexanderHaas, Ali azad bakhsh, Alla tedesa, Amccord, Andre Engels, AndrewHowse, Andryono, Angelo Michael, Auric, Bhadani, Biscuittin, Bjankuloski06en, Bkell, Bluemoose, Bobo192, Brandmeister (old), C.Fred, Carl.bunderson, Carmichael, Chavez83, Clicketyclack, Cwolfsheep, Daabomb, David Moerike, Dawnseeker2000, Deez Nut\$, Doctorknock, Drewzhradogue, DropDeadGorgias, Duncan, Dwight666, EagleOne, EdwinHJ, Eeekster, Erwinrossen, Espero, Fighting for Justice, Flurry, Fudge55, Gbrownlee, Gemshine31, Glenn, Gman2337, GraemeL, Gtwfan52, Guaka, Gurch, Guy Harris, HamburgerRadio, Harryzilber, Henry W. Schmitt, Henrymxr, Hillcrest, Hu12, Ilyacg, Interik, Itai, Jamesofur, Jdenning55, Jeex78, Jehochman, Jennymorley, JeremyA, Jfmantis, Jhbteil, Jim.henderson, Jimiruin, Jnavas, Joyous!, Julianhall, KVDP, Kbrose, KelleyCook, Kentucky jack, Kgr, Khazar, Kocio, Kurtik, LeaveSleaves, Leon7, Lewisskinner, LittleWink, Llywrch, LorenzoB, Lzur, MER-C, Mac, Madhero88, Markeilz, Martin451, Maxxdxx, Mlaffs, Mortense, Mwanner, Nealmcb, Netsnipe, Niciegued, NickBush24, NightingaleJ, Nnp, Nulkilusumin, Ohnoitsjamie, OlEnglish, Omegatron, Oterdude, Pawarol, Pearle, Petergargano, Pkg, Phil Boswell, PhilKnight, Philip Trueman, Pigsonthewing, Piroget, Playmobilishorse, Pnm, Polkaspost, Postdlf, Puggs, Racklever, Raghuvanshi86, Rahulmkhj, Raistlin11325, Redrocket, Redvers, Requestion, Rjwilmsi, Roastytoast, Robo56, Rory096, Satanhimself666, SchuminWeb, Sean Reynolds, Sfz, Silvery, SimonP, Sinher, Sjö, Skapur, Smack, Snafflekid, Snigbrook, SoWhyy, Some jerk on the Internet, Sonofzepp, Starwind Amada, Stephan Leeds, Supergyro2k, T Cuzzillo, Techxact, Tedernst, Teebone, Terjen, TheIrishWarden, Thumperward, Tide rolls, Tobixen, Tomclark, Tow, Towel401, TreasuryTag, Ukexpat, Uncle G, ValC, Veinor, Vince7133, Vrenator, Waggers, Warwickcaddie, Whotspot02, William Avery, Woohookitty, Xavexgoem, Zanter, 417 anonymous edits

**OSI model** Source: <http://en.wikipedia.org/w/index.php?oldid=509796095> Contributors: 0612, 0x6D667061, 1337 JN, 1966batfan, 24.12.199.xxx, 28bytes, 336, 63.227.96.xxx, 7, 75th Trombone, 802geek, 90 Auto, @modi, A412, A930913, ABF, Abarry, Abune, Adamantians, Addshore, Adibop, Adityagaur 7, Adj08, Adoniscik, Adrianwn, Advancedtelcov, Aageekgal, Ahoerstemeier, Aitias, Ajo Mama, Ajw901, Alansohn, Albanoaco, Aldie, Ale jr, AlistairMcMillan, Allens, Alphachimp, Alucard 16, Alvestrand, Amillar, Amitbhatisa76, Amtanoli, Andjohn2000, Andre Engels, Andybryant, Angryskochop, Animum, Anjola, AnkhMorpork, Anna Lincoln, Anon lynx, Anonymous anonymous, Another-anomaly, Apocryphie, Apparition11, Arroww, Artur Perwenis, Arunachalammanohar, Ashutosh.mcse, Aslambasha09, Asn1tv, AtomicDragon, Atreyu42, Audunv, Avitesh, AxelBoldt, Ayengar, B4hand, BACbKA, BDerrly, Bakilas, Balajia82, Bariswheel, Bchiap, Bdamokos, Beelaj, BenLiyanage, Beno1000, Biblbroks, Bjelleklang, Bletch, Blueskies238, Bmylez, Bobo192, Bogdangiuse, Boikej, Bojer, BonmelDing, Bonobosarenicer, Booyabazooka, Borgx, Brambleclawx, Brandon, Brick Thrower, Brougham96, Bryan Derksen, BuickCenturyDriver, Bzimage.it, Bücherwürmlein, CDima, Clreland, CMBJ, Caerwine, Caesura, Calmer Waters, Caltas, CambridgeBayWeather, Camw, Can You Prove that You're Human, Can't sleep, clown will eat me, CanadianLinuxUser, Cand4c, Caper13, Carre, Casey Abell, Causa sui, Chburnett, Cbustapeck, CfIm001, Charles Edward, Charm, Che090572, Chester Markel, Chfalcio, Chimpx, Chirag, Chrislk02, Chupon, Cikedragan, Citcat, Closedmouth, Cokoli, Cometstyles, Conquest ace, Conversion script, Coriron, Courcelles, Cptudoc, CraSH, CraigBox, Crasheral, Crimsonmargarine, Cs mat3, Cibolt, Cxxl, Cybercobra, CyborgTosser, Cykt sui, CynicalMe, DARTH SIDIOUS 2, DJPholy, DSparillo, Damian Yerrick, Daniel, Danlev, Dave2, Davetrainer, David Edgar, David Gerard, David0811, DavidBaral, DavidLevinson, DavidJ, Dcooper, Dcovell, Deagle AP, Delfeye, Delldot, DeltaQuad, Demitsu, Denisaron, DennyColt, Dgtsyb, Dicklyon, Dili, Dino.korah, Discospinster, Dispenser, Djib, Djmoa, DmitryKo, Dmohantyatgmail, Doniago, Dparc, DrDOS, DrSpice, Drat, Dreish, Drwarpmind, Duey111, Dumbledad, Dzubint, EJDyksen, EJSawyer, ENeville, EagleOne, Easy007, Ed g2s, EdH, Edvorce, Edward, ElKevbo, Eldiablo, Eleassar, Elfosardo, Eliezer, Elipongo, Emperorbma, EnOreg, Enjoi4586, Enochlau, Ebpr123, Eric Soyke, Everyking, Evillawngnone, Ewyahooocom, Excirial, FF2010, Falk.H.G., Fang Aili, Feezo, Fiable, BiZ, Filemon, Finlay McWalter, Fijama, Fleg31789, Flewis, Flowanda, Fraggle181, FrankTobia, Fred Bradstadt, Fredrik, Free Bear, FreshPrinz, Freshenees, Friday, Friedo, Friginator, Fullstop, Fumitol, Fuzheado, Fvw, Fæ, GGShinobi, Gadfiuum, Gafex, GarethGilson, Gary King, Gaspol, Gazpacho, Geek2003, General Rommel, Ghostalker, Giftlite, Gilliam, GlassCobra, Glenn, Goodnightmush, Graeme Bartlett, Grafen, Graham.rellinger, GreYFoXGTi, Grendelkan, Grubber, Gsl, Gurchzilla, Guy Harris, Gwernol, Gökhann, H2g2bob, H34d, HMGb, Haakon, Hadal, HamatoKameko, HarisM, Hatch68, Heberkowitz, Hdante, Helix84, Hellomarius, Henrikholm, Heron, Hes Nikke, Hetar, HexaChord, Hgerstung,

Hiddekel, Highpriority, Honeyman, I dream of horses, IMSoP, IReceivedDeathThreats, Iambk, Iambossatghari, Ideoplex, Ifroggie, Ilario, Immunize, Inkhorn, Inkling, Insineratehymn, Intgr, Inversetime, InvisibleK, Inwind, Iridescent, IronGargoyle, Ishikawa Minoru, Island Monkey, Isofox, Isthishingworking, Itpastorn, Itusg15q4user, Iviney, J.delanoy, JMatthews, JV Smithy, Jake Wartenberg, JamesBWatson, Jannetta, Jatinisinha, Jauerback, Jchristn, Jcw69, Jdrrmk, JeTataMe, Jeanjour, Jeff G., Jeffrey Mall, Jessemerriman, Jetekus, Jhilving, JidGom, Jim1138, Jimw338, Jjenkins5123, Jmorgan, Jnc, JoanneB, JodyB, Joebeone, John Hopley, John Vandenberg, John254, Johnblade, Johnleemk, Johnuniq, JonHarder, Jonathanwagner, Jonwatson, Joodas, Josef Sábl cz, Josh Parris, Jovianeye, Joy, Jpta, Jrodor, Jschmnr, Jscloon4, Jsonheld, Jusdfax, Kaaveh Ahangar, Kallaspriti, Karelklic, Karpouzi, Kaszeta, Katalaveno, Kaz219, Kazrak, Kbrose, Kcordina, KerrVeenstra, Kesla, Kevin Rector, Kgrr, Khat17, Killionduude, Kim Rubin, Kingpin13, Kirill Lokshin, Kkbairi, KnowledgeOfSelf, Kraftlos, Kramerino, Krampo, Krellis, Kuru, Kvng, Kyllys, LOL, LOTRrules, Lachlancooper, Lankiveil, Lawrence Cohen, Lazarus666, Leafyplant, Lear's Fool, Lectonor, Lee Carre, Lights, LittleOldMe, LittleWink, LizardJr8, Lockcole, Logitheo, Logthis, Lomn, Looxix, Lord Chamberlain, the Renowned, Lordeaswar, Lotje, Lulu of the Lotus-Eaters, Luna Santin, Lupin, Lynnallendaly, M, MBisanz, MER-C, MIT Trekkie, Maguscrowley, Mahanga, Mahesh Sarmalkar, Majorly, Mange01, Manishar us, Marek69, MarkSutton, MarkWahl, Markb, Markhurd, Markolinsky, MartinHarper, Martinkop, Marvin01, Materialscientist, Mattalyst, Matthew Yeager, Mattjgalloway, Mattmill30, Mbc362, Mboverload, McGinnis, Mcnuttj, Mdd, MEEPster, MelbourneStar, Mendel, Mephistophelian, Merlin444, Metaclassing, Micahcowan, Michael Hardy, Michael miceli, Mike Rosoft, Mikal Ward, Mikeo, Mikeyh56, Milind m2255, Minimac, Mkweisse, Mlewiss000, Mmeerman, Mmernex, Mmmeg, Mobius R, Mohitjoshi999, Mohitsport, Mojalefa247, Monterey Bay, Morten, Moxfyre, Mr Elmo, Mr Stephen, Mr.ghilan, MrOllie, Mrankur, MrsValdry, Mtd2006, MuZemike, Mudasir011, Mulad, Mwtowers, Myanw, Myheadspinsincircles, N-Man, N5iln, Naishadh, Nanshu, Naohiro19, Naresj angra, Nasa-verve, Natarajabu, Nete Silva, Nathashashleywild, NawlinWiki, Nbarth, Nbbatla, Neevan9, Nejko, Nemesis of Reason, Nethigirb, Netsnipe, Niaz, Nick, Nickshanks, Nicolas1981, Nisavid, Nitecruzr, Nivix, Nk, Nkansahrexford, Noahspurrier, Nolyann, Nsaa, Nubiotech, NuclearWarfare, Nux, OSUKid7, Octahedron80, Odie5533, Ogress, Oita2001, OIEnglish, Omnicronperse8, Orange Suede Sofa, Ore4444, Originalharry, Ott, Ottosmo, Ouishiobean, Oxymoron83, PGWG, Palltrast, Pamri, Panser Born, Paparodo, Parakalo, Pastore Italy, Patch1103, Patrikor, Patstuart, Paul August, PaulWIKIJeffery, Payal1234, Pb30, Peni, Penno, Pethr, Petr, Phatom87, Phil Boswell, Philip Trueman, PhilipMW, Pluoy8999, Pmorkert, Pointillist, Postdlf, Postmortemjapan, Praggu, ProPuke, Pseudomonas, Psiphior, Public Menace, Puchiko, Puckly, PyreneesJIM, Pytomm, RainbowOfLight, Raju5134, RandomAct, Ravikiran r, RazorICE, Reannon100, Rebroad, Recognition, RedWolf, Reedy, Rejax, Rettetast, Rfc1394, Rgilmchrist, Rhobite, Rich Farmbrugh, RichardVeryard, Richwales, Rick Sidwell, Rjgodoy, Rjstinye, Raager, Rnb, RobEby, Robert K S, RobertL30, RockMFR, Rohwigan03, Ronz, Roo314159, RoscoMck, RossPatterson, Roux, Roux-HG, RoyBoy, Rsiddharth, Runis57, RuntuX, Rurus, Ryan au, Ryt, Ryulong, S, S3000, SMC, Saad ziyad, Saddy Dumpington, Safety Cap, Saintfiends, Sakurambo, Savh, SaxicolousOne, Scarian, Schumi555, Scientus, Scobhoust, Scolobb, Scottonsocks, Seaphoto, Sesu Prime, Shadow1, Shadowjams, SharePointStacy, Shell Kinney, Shirik, Shoeofdeath, ShornAssociates, Shradhha deshmukh, Shrofami, Sietes Snel, Simonfl, Simple Bob, SineChristoNon, Sir Nicholas de Mimsy-Porpington, Skier Dude, Sliceofmiami, Slroberton, Smalljim, Smokizzy, SnowFire, Snowolf, Soosed, Sp33dyphl, SpaceFlight89, Speaker to Lampposts, SpeedyGonsales, Spitfire8520, SpuriousQ, Srived, StaticGull, Stemonitis, Stephan Leeds, Stephen Gilbert, StephenFalken, Stevage, Steven Zhang, StuartBrady, Subfrowns, Sunilmalik1107, Surueuna, Suyashparp, Swapcouch, Syntaxsystem, TAS, THEN WHO WAS PHONE?, Tagishsimon, Tangotango, Tarekradi, Taruntan, Tbsdy lives, Tencv, Techtoucian, Tedickey, Tellyaddict, Tempodivalse, The Anome, The Athlon Duster, The Haunted Angel, The Thing That Should Not Be, Therumakna, Thief12, Thingg, Think4amit, ThreeDee912, ThunderBird, Tide rolls, Tin Q, Wells, TinyTimZamboni, Tom harrison, TomPhil, Tommy2010, Tompsc, Tony1, Tooki, Tpbtradbury, Tpvibes, Tranzz, Travelbird, Tree Biting Conspiracy, Trevor MacInnis, Triona, TripleF, Triwbe, Troy 07, Turb0chrg, Tyler.szabo, UU, Umair ahmed123, Uncle Dick, Unkownkid123, Venu62, Versus22, VidGa, Vishnava, Visor, Vn anantha, Vimgrupurash, Voidxor, WLW, Waggers, Warrierekash, Wayfarer, Weregerbil, Whitejay251, WikiDan61, Wikipelli, William Avery, Willking1979, Wilson.canadian, Wily duck, Wingman417, Winston Chuen-Shih Yang, Wire323, Wireless friend, Wishington, Wknight94, WoiKICK, Woohookitty, Wrlee, Wrs1864, Wtmitchell, Witshymanski, Yamamoto Ichiro, YamiKaitou, Yamike, Yms, YolanCh, Yuuko112, ZX81, ZachPruckowski, Zachary, Zoobee79, İluman, 3251 anonymous edits

**Physical Layer** *Source:* <http://en.wikipedia.org/w/index.php?oldid=469748889> *Contributors:* 1exec1, AGruntsJaggon, Acdx, Alai, Alfio, Amaurea, Amillar, Amire80, Arastcp, Arnero, BD2412, BertK, BjKa, Borgx, Bouquet, Brest, Butko, CONFIQ, CanadianLinuxUser, CannonR, Carl.bunderson, Cfrost, Chriscandy, Clovis Sangrail, CosineKitty, DerHexer, Deville, Dgtsyb, Dicklyon, Digisus, Dkovacs, Dominio, Drieken, Digm, Eastlaw, EdH, Emperorbma, EnOreg, Enjoi4586, Epbr123, Europrobe, Extraordinary, Fahidka, Gary63, Gcharles, Gerixau, Giftlite, Giraffedata, Grafen, Grassynel, Green8907, Grendelhan, Guy Harris, Harobikes34, Harp, Hede2000, Henry Stanley, Hetar, Hosterweis, IMC Networks, Ian99, Ibarrere, ImpossibleEcho, IntrigueBlue, Inwind, Itai, Itpastorn, Itusg15q4user, Jafeluv, James smith2, John Silvestri, Johnuniq, Jredmond, Kaaveh Ahangar, Kbrose, KelleyCook, Kevin Rector, Kremso, Kubanczyk, Kvng, Lawrence Cohen, Leszek Jańczuk, Linkminer, Lmatt, Looxix, Lord Chamberlain, the Renowned, Luckyherb, Mange01, Marianocewski, Marketsnipers, Martarius, MartinHarper, Mbhy87, Mlewiss000, Mosca, Nbartz, Nubiotech, NyAp, PaulTanenbaum, Pepsi Lite, Phantasee, Phoenix-forgotten, Pinethicket, RexNL, Rick Sidwell, RockMFR, Rwwww, SatyrTN, Savannah Kaylee, SchreyP, Scootey, ScottDavis, Shashiranjan18, Sietse Snel, Slamminheads, Stdazi, Ta bu shi da yu, Tagishsimon, Template namespace initialisation script, TimothyJKeller, Tomchiukc, Tsuite, UU, Underpants, Violask81976, Wbwm1058, Welsley, Widefox, Yacht, Yyy, 162 anonymous edits

**Media Access Control** *Source:* <http://en.wikipedia.org/w/index.php?oldid=459009207> *Contributors:* @modi, A purple wikiuser, Alexander.stohr, Angela, Arathald, Arkrishna, Avitesh, Beno1000, Bentogoa, Borgx, Breno, Caesura, Casey Abell, Cburnett, Closedmouth, Crazy Murdoc, Dawnseeker2000, DenesVadasz, Dgtsyb, Dicklyon, Dombinio, Ebraminio, Enjoi4586, ErikHaugen, Evercat, Extraordinary, FDD, Figureskatingfan, GPHemsley, Ghez, Giftlite, Good Olfactory, Gwalker nz, HappyCamper, HarisM, Intgr, Irmavash, Itai, JFSM, Jesse Viviano, JocConnor, Johnuniq, Jusdfax, Kbrose, KelleyCook, Khazar, KnightRider, Leon Hunt, Lihu912, Logan, Loosecannon93, Luis Felipe Braga, Mange01, Mellery, Mlaffs, Mojodaddy, Mr Stephen, Nageh, Notheruser, Nuno Tavares, Nur, OrangeDoe, PaulTanenbaum, Pgallert, Philip Trueman, Proveit, Rick Sidwell, Snori, Srlleffler, Stassats, Steven Hepting, Suruena, Template namespace initialisation script, Timwi, Treekids, Vitz-RS, Widefox, Willy on Wheels over Ethernet, Woohookitty, Youssefsan, Zachipliton, Zanetu, Zoicon5, 113 anonymous edits

**Logical Link Control** *Source:* <http://en.wikipedia.org/w/index.php?oldid=459011673> *Contributors:* Alcmaeonid, Anrie Nord, BaomoVW, Bearcat, Beno1000, Borgx, ChesterMarkel, Dgtsyb, Dicklyon, Discospinster, Doulos Christos, ErikHaugen, Frap, Fsiler, GermanX, Good Olfactory, Guy Harris, Hgfaren, Indil, Inwind, Itusg15q4user, Karthick.s5, Kauczuk, Kbrose, KelleyCook, Krmboya, Laurusnobilis, Mange01, Materialscientist, Muhandes, Od Mishehu, PaulTanenbaum, Pgallert, Phatom87, Ppcailley, Qnoonus, The Anome, Very Input, Wayfarer, Widefox, Ysangkok, 56 anonymous edits

**Data Link Layer** *Source:* <http://en.wikipedia.org/w/index.php?oldid=469748925> *Contributors:* 1000Faces, 3DS Mike, AAA!, AGruntsJaggon, Aldie, AlexandriNo, Alfio, Amillar, Angela, Arastep, B4hand, Barri, BigDunc, Blehfu, Butko, Cahover, Canterbury Tail, Casey Abell, Cgelpi3, Crispmuncher, DanMS, DavidABraun, Dddddd2w32, Dgtsyb, Dicklyon, Diogenes00, Docu, Dominio, Eekoo, Egil, Ehn, Ekabbishiek, Ember of Light, EnOreg, Enjoi4586, Excrial, Falkony, Gasheadsteve, Geek2003, Giftlite, Guy Harris, Hadal, Hede2000, Ibarrere, Intgr, Invictus42, Inwind, Itai, Itpastorn, Itusg15q4user, Jafeluv, James smith2, Jmkim dot com, Johnuniq, Kannadigahavi, Kbrose, Ken I lee, Kjetil r, Konstable, Kubanczyk, Lawrence Cohen, Looxix, Lsukari, Luis Felipe Braga, Mange01, MartinJ Hoekstra, MartinHarper, Mattheumeguire, Michael Hardy, Mplearce, Nixdorf, Nolispanno, Numa, Oli Filth, Omargamil, PaulTanenbaum, Philip Trueman, Plasticup, Playstationman, Rabarberski, Ravensun, Rscrinter123, RedWolf, Remember the dot, Rick Sidwell, SatyrTN, ScottDavis, Shanel, Shiro jdn, Sin-man, SirPavlova ♥, SkipHuffman, SpaceFlight89, Sross (Public Policy), Stdazi, Suruena, Talinus, Template namespace initialisation script, TexasAndroid, TheFeds, Thierry, Tide rolls, Timo Honkasalo, Toccata quarta, Tomchiukc, TripleF, Turian, TutterMouse, Uduunuwaru, WLW, Webgeek, Weregerbil, Why Not A Duck, Widefox, Willy on Wheels over Ethernet, Wplacek, Yacht, Yyy, ZeWrestler, Zfr, Tiveropolinik, 178 anonymous edits

**Network Layer** *Source:* <http://en.wikipedia.org/w/index.php?oldid=469748958> *Contributors:* Abhi 4442003, Adrian M. H., Alain.ternette, Alfio, Arastcp, Arnavchaudhary, Arunachalammanohar, Ashishindeman, Bendykst, Borgx, Butko, Capricorn42, Chereekandy, Colin Marquardt, Crawdaddio, Dgtsyb, Dicklyon, Digisus, Dominio, Dribbleboy, Dthomsen8, Egret, Elkvebo, EnOreg, Enchanter, Enjoi4586, Enochlau, Epbr123, Feezo, Fredrik, Geek2003, Giftlite, Goatasaur, Gouldja, GringoCroco, Haakon, Hede2000, Igoldest, Immibis, Infrogmation, JCWilson, Jafeluv, James smith2, Jgiam, Jim1138, Jnc, Johnuniq, Jorge Stolfi, Josh Parris, Karith, Kbrose, Kvng, Lankiveil, Looxix, MajorFreakinEnglish, Mange01, Mark7-2, MartinHarper, Mbhy87, Muhammed Salman Jamal, Muhandes, NYMets2000, Nathan Hamblen, Niteowneils, Nixdorf, Oscartheeat, PaulTanenbaum, Pepsi Lite, QuadrivialMind, RazorICE, Rick Sidwell, RobertMfromLI, SatyrTN, ScottDavis, Strake, Template namespace initialisation script, Tompagenet, Widefox, Woohookitty, Yacht, Zac439, 140 anonymous edits

**Transport Layer** *Source:* <http://en.wikipedia.org/w/index.php?oldid=469748993> *Contributors:* 1ForTheMoney, Adonikin, Alansohn, Aldie, AlistairMcMillan, Altenmann, Alvestrand, Andrew Hampe, Andreyf, BenBreen2003, Bigmantonly, Borgx, Brettmeleys, Butko, Butlern, Choudesh, Conan, Costello, Dgreen34, Dgtsyb, Dzlinker, Eggnock, EnOreg, Enjoi4586, FatalError, Fmunsch, Fred Bradstadt, Gavinatkinson, GermanX, Giftlite, Guy Harris, Hadal, Hede2000, Highlandsun, Hullbr3ach, Imcdnlz, In21h, Inwind, Ipatriol, Jdelanoy, JHolman, Jafeluv, Jec, Jimfbleak, Jnc, Johnuniq, Kadin2048, Kbrolino, Kbrose, Kingpin13, Kkdkc, Kungfuadam, Kvng, Kwi, LiDaobing, Limbo socrates, Looxix, Lost.goblin, MTC, Mange01, Marcan, MartinHarper, Mirv, Mmmready, Nealmcb, Nixdorf, Ovy, Phantomsteve, Phatom87, PrologFan, Quibik, Razorflame, Retroguy90, Rmhermen, Robth, Samjoopin, SatyrTN, ScottDavis, Simon04, Suffusion of Yellow, Suruena, Tcmcfaul, Template namespace initialisation script, Tpvibes, Vipinhar, Wmasterj, Yacht, Yyy, Zac439, ZeroOne, Zoicon5, 147 anonymous edits

**Session Layer** *Source:* <http://en.wikipedia.org/w/index.php?oldid=469749033> *Contributors:* Alan.tate, Aldie, AlistairMcMillan, Arastep, Bald Zebra, Borgx, Btorrnado, Butko, CecilWard, Conti, Danielcohn, Dgtsyb, Digisus, Dontopenyoureyes, Eleassar, EnOreg, Enjoi4586, FelipeVargasRigo, Fred Bradstadt, Frood, GLaDOS, Gbeeker, Giftlite, Guy Harris, Hede2000, J.Tame, JHolman, Jafeluv, James smith2, Jamesooders, Jll, Johnuniq, Jonathan Drain, Kbrose, Kris Schnie, LFaraone, LOLEDITING, LiDaobing, Looxix, Mange01, MartinHarper, Mav, MementoVivere, Nisiguti, Oli Filth, PaulTanenbaum, RedWolf, Rick Sidwell, SD5, SatyrTN, ScottDavis, Shiro jdn, Stdazi, Template namespace initialisation script, Tinnitus97, Tobias Conradi, Underpants, Widefox, Yacht, Tiveropolinik, 66 anonymous edits

**Presentation Layer** *Source:* <http://en.wikipedia.org/w/index.php?oldid=469748821> *Contributors:* ACSE, Alan Pascoe, AlistairMcMillan, Anon lynx, Arastcp, B4hand, Bchiap, Bkell, Borgx, Butko, CyborgTosser, Danielcohn, Dgtsyb, Digisus, EagleOne, Ebobjr, EnOreg, Enjoi4586, Facuq, FelipeVargasRigo, Francs2000, Gmlk, Guy Harris, Hede2000, Hetar, Itai, Jafeluv, James smith2, Jelsova, Jengellh, Jnc, Jotel, Kbrose, Keegscee, Khendon, Kremso, LiDaobing, Looxix, MartinHarper, Michael Hardy, Modster, Nisiguti, Orderud, PaulTanenbaum, Ravensun, RedWolf, Rjgodoj, SatyrTN, ScottDavis, Sdfisher, Shad0wfyr3, Shanes, Sross (Public Policy), Stdazi, Template namespace initialisation script, The Grumpy Hacker, Timsk, Ugur Basak, Underpants, W Nowicki, Widefox, Yacht, Yunshui, Zap Rowsdower, 64 anonymous edits

**Application Layer** *Source:* <http://en.wikipedia.org/w/index.php?oldid=469748861> *Contributors:* AS, Ahoerstermeier, AlistairMcMillan, Amillar, AndyHedges, Arunachalammanohar, Ashdurbat, B4hand, Bearcat, Brest, Butko, ChazBeckett, Cradel, DDR2Nite, Dlonized, Danim, DeweyQ, Dgtsyb, Dicklyon, Dogcow, Dominio, Eimsand, Ejabberd, ElKevbo, Enjoi4586, Evertw,

Fetoma, Frap, Fredrik, Geozapf, GermanX, Gilliam, Graham87, GrapeSteinbeck, Graph, Gruzd, Harryboyles, Hawaiiboy99, Hede2000, Honcw, Hrvoje Simic, Hu12, Ipahopehead, IvanLanin, Jafeluv, James smith2, Jamie, Jauerback, Jaybeeunix, Jaymcjay, Jerome Charles Potts, Jnc, Johnuniq, Jorunn, Kbrose, Kbthompson, Kesac, Lababidi, LiDaobing, Looxix, Lost.goblin, Lulu of the Lotus-Eaters, Lysdexia, MainFrame, Mange01, Markushx, MartinHarper, MattieTK, Mfloryan, Mbby87, Minesweeper, Morte, MrsValdry, MulberryBeacon, Mwtewe, Nhorton, Night Gyr, Nixdorf, Orphan Wiki, Oxymoron83, Panarchy, Pelleasaphnis, Pgallert, QueBurro, R'n'B, Ramprasad.ap, Reconsider the static, RedWolf, Rich Farmbrough, Rserpool, SatyrTN, Schlesselman, ScottDavis, Shii, Squideshi, Stephan Leeds, Stonehead, Stryn, Suruena, Template namespace initialisation script, Tmopkisn, Useight, West.andrew.g, Wisamsafi, Wknight94, Wmasterj, Yacht, Yerpo, Zac439, Zfr, أَمْدَهُ مُصَفِّي السَّبَدِ, 174 anonymous edits

**IEEE 802.1D** *Source:* <http://en.wikipedia.org/w/index.php?oldid=499160638> *Contributors:* Alvestrand, Alynna Kasmira, Avij, Geek2003, Giftlite, KelleyCook, Kgrr, Kvng, L736E, Lars T., Mdito, PigFlu Oink, Plugwash, Stephan Leeds, 10 anonymous edits

**Link Layer Discovery Protocol** *Source:* <http://en.wikipedia.org/w/index.php?oldid=499460010> *Contributors:* 0x6adb015, AlexandriNo, Alvin-cs, David McBride, Dethomas, Dyork, Electron9, Gerald.combs, HammondJr, Jdparker520, KJS77, Kbrose, KelleyCook, Kvng, Kwamikagami, Markelrick, Muchris, Naveenpf, Pgr94, Saurabhpal, Terry.simons, The Thing That Should Not Be, ZorroII, 51 anonymous edits

**Spanning tree protocol** *Source:* <http://en.wikipedia.org/w/index.php?oldid=424043401> *Contributors:* 7, ABF, Aaron.hebert, AaronSw, Abrech, Abune, AdrianSuter, Aldie, Altenmann, Alvestrand, Alvin-cs, Ant1357, Anthony Appleyard, Apjha, Apps123, Arnaud, Atigala2003, B4hand, Baccala@freesoft.org, Banej, BartonM, Bellenion, Bellhead, Bergon, Blatkinson, Bongwarrior, Booyabazooka, Boscobiscotti, Bryan Derksen, Bstpiere, CALR, CableCat, Capricorn42, Charlies, CrashJunkee, Davepave, David Epstein, Dicklyon, Dirk gently, Dominus, Dysprosia, DÉRahier, Eaderhold, ESkog, Easwamo1, Echoray, Edurant, Ellery, Emurphy42, Epbr123, Eug, Everyking, Evyn, Fabriciodosanjossilva, FlyingToaster, ForthOK, Frank, FrankTobia, Friday, Galoubet, Gardar Rurak, Geek2003, Ghettoblaster, Ghewgill, Ghost, Giraffedata, Glass Sword, Grafen, Guy Harris, Habbie, Harshilyas, Hendersonnv, HorsePunchKid, Ilario, Irmatov, Ixfd64, J.delaney, Jeffq, Jeroen, Jesse Viviano, Jkl, JonHarder, Joseane, Kai-Hendrik, Kaushal.shaky, Kb, KelleyCook, Kgrr, Krellis, Kvng, Larry Yuma, Lee Carre, Lhmathies, Limowreck, Lingathoor, Lotje, MER-C, MLD7865 Auto, MadSurgeon, Mchadlock, Meicogni, Mephistophelian, Michael Hardy, Michael Sloane, Mikens22, Miketubby, Mincebert, Minna Sora no Shita, Mmeerman, N3rV3, Negrulio, Ngriffeth, Nickfox, Nuno Tavares, Os87, P0Or, Palthaino, Pdpatil, Pgallert, Pgr94, Phisches, Plugwash, Pimaccabe, Pmj, Pnm, Populus, PsyberS, RJHall, Radagas183, Rafterman, Redfeamb, Rednectar.chris, Reinderien, Rjwilmis, RockMFR, Salesms19, Sanddune00, Sceptre, Scobra77, SeanDague, Seanx820, Shahid789, Skandha101, Skier Dude, Siccias, Stagira, Stephan Leeds, Stryqx, Suruena, Tfdb, The Thing That Should Not Be, The emm, Tige, Timwi, Tinucherian, Tkteun, Tofergregg, Tonkie, Triddle, UncleBubba, Vlhsp, Weirdy, WikiReviewer.de, Wk muriithi, Yellowking, Yidisheiry, Zack, Zigger, 356 anonymous edits

**IEEE 802.1p** *Source:* <http://en.wikipedia.org/w/index.php?oldid=381995024> *Contributors:* Boism, Bulwersator, Eyreland, Guy Harris, Isidrov, JonHarder, Kasshyk, KelleyCook, Kvng, Martarius, Martinwilke1980, Mokhtari, Nasa-verve, Pagingmrherman, Palfrey, Schlegel, Smallpond, Steven Hepting, Widefox, 27 anonymous edits

**IEEE 802.1Q** *Source:* <http://en.wikipedia.org/w/index.php?oldid=502964564> *Contributors:* Aleksey Gerasimov, AlessandroPoggi1973, Alter-alter, Angusmc, Anon lynx, Arkrishna, BenAveling, Bezenek, Biot, C8h1Ino2, CesarB, ChrisCPearson, Curtmed, Danhash, Daniel.jaro, DanielLeicht, Devijethye, Filipvre, Gaius Cornelius, Ginger18, Guy Harris, Ibc111, Infofarmer, Itai, Jamelan, Joy, Jrp, Kbrose, KelleyCook, Kvng, Leangjia, MTurpin, Mattyli, Mdito, MessifCB, Mmxn, Mulad, Pb30, Pgallert, Plugwash, Quinxorin, Raanoo, Radioscout, Rchandra, Rednectar.chris, Richard0612, Rick Sidwell, RI, Robparten, Rusty Cashman, Saaga, Scorpious, Sebastian Goll, Shmelyova, Sietse Snel, Sreeakshay, Stefan Bethke, Stormrose, Suruena, Tas50, Technobadger, TelecomNut, Zehawk, 109 anonymous edits

**IEEE 802.1X** *Source:* <http://en.wikipedia.org/w/index.php?oldid=506379258> *Contributors:* Alex.muller, Arr2036, Austin512, Brianmarsden, CALR, Chasmo, Damian Yerrick, Dawnseeker2000, Derek Balsam, Dysprosia, Excirial, Fethers, FlippyFlink, Frol, Furlong, Ghettoblaster, Gilliam, HawseK, Hellisp, Henkk78, Hooligan6, Hunding, Int21h, Isidore, Itai, Iuhkhjhk87y678, Jag123, Jedimike, Jiraffe, Jonbrition, Jrp, Jtm169, JuanpdP, KelleyCook, Kgrr, Koumoula, Kvng, Lostowl05661, Magioladitis, Martarius, Matt Crypto, Mdito, Mespinola, Mgri, Nabla, Nasa-verve, NoobX, Paulehoffman, Pnm, Povlhp, R'n'B, RaseaC, Requestion, Rgisraelsen, Ruleke, Salvio giuliano, Sceptre, Scott.somohano, Suruena, Thandor, TiCPU, Tmh, Vodonokone4, Voidxor, Wxavyriver, Wlgrin, Xpclient, Yaronf, 218 anonymous edits

**Ethernet** *Source:* <http://en.wikipedia.org/w/index.php?oldid=508507054> *Contributors:* 0612, 121a0012, Ilovegal, 1stJahman, 4a6f656c, 7, ARC Gritt, Aapo Laitinen, Abdull, Adashiel, AdjustShift, Adrian.benko, Aeluwas, Ahoerstemeier, Ajraddatz, Akriasas, Alan Lieffing, Alansohn, Aldie, Ale jrb, Alecv, Algocu, AlistairMcMillan, AlterMike, Alvestrand, Alyssapry, Amatulic, Ameliorate!, Amillar, Amore proprio, Anaraug, Andareed, Andreas Toth, Andy Dingley, Andybryant, Andyhodapp, Aneah, Angela, Angusmc, Anss123, Applemacintosh10, Arch dude, Arkrishna, Armando, ArnoldReinhold, Artaxiad, AtomEdge, Avono, Azghal of Belegost, B4hand, BD2412, Bbachrac, Bctrwriter, Bdmcmaoh, Bccritical, Betacommand, Betbest1, BiT, Bidabadi, Bigbogmcgee, Bigjimm, Bilbo1507, Biot, BlueAg09, Blutrot, Bobblewik, Boffy b, Bonmac, Bookbrad, Bookofjude, Bootlegglingy mcbootleg, Boscobiscotti, Bovineome, Branclem, Branko, Brian Patric, BruceLee, Btilm, Bumm13, Buy P%E%P%\$%, CñanPayne, CRGreathouse, CS46, Calltech, Caltas, CamTarn, Can't sleep, clown will eat me, Capricorn42, CarloJerna, Casey Abel, Catgut, Causantin, Chburnett, CesarB, Chaogsate, Charles Gaudette, Chasingols, Chealer, Chmod007, Chowbok, Cdaniel, ClementSeveillac, Closedmouth, CloudNine, Cluth, Cmdrjameson, Colin Marquardt, Conversion script, CorpX, Corti, Corwin8, Cpl Syx, Creidieki, Crispnuncher, Crissov, CryptoDerk, Cstanners, Cybercobra, DVdm, Daa89563, Dachshund, Damiani Yerrick, Davehead, David Biddulph, DavidBailey, DavidH, Dcorzine, Deflective, Dennis Brown, Dicklyon, Digitalsushi, Discospincter, Diskdoc, DocWatson42, Dogcow, Donnieefarrow, Download, Drak2, Drphiharmonic, Dtcldhingy, EEfirl18, EagleOne, Ebear422, Econrad, Eeekster, Efa, Egil, Ehni, Eivind F Øyangen, El Cubano, ElBenevolente, Electron9, Elektrik Shoos, Eleuther, Elmrbuy, Eloil, Engineermist, Enjo14586, EgGuy, Epbr123, Evil genius, Ewlyahocom, Excirial, Facts707, Femto, Fenrisul, Fetofs, Fieldday-sunday, Finest1, Firsfron, Flewis, FocalPoint, Frankchn, Frap, Fratrep, Fred Bradstadt, Fredrik, Freshenees, Fudoreaper, Fulldcent, Furykef, G4wsz, GTAKillerEric, Gah4, Gascreed, Geek2003, Gekkoblaster, Generica, Ghaly, Giflite, GlacialFox, Glenn, Gnalk, Gnuish, Gogo Dodo, Golgofrinchian, Gopher23, Goplats, Gousub, Graham87, Grandsonofmaiden, Greylion, Grgan, Guanxi, Guy Harris, Gyankhawani, H0serdunde, HCelic, Haakon, Hadal, HappyCamper, Hayzilber, Harvester, Helix84, Herborther, Heron, Hobophobe, Hughey, Hungrymouse, Hussein95, Hvn0413, Iambk, Iamzemasterraf, Ibc111, Idkyididthis, Igoldste, Indefatigable, Ingr, Irdescent, Iqr, Isaac Rabinovitch, Itai, Itusg15q4user, J.delaney, J04n, Jakohn, JamesBWatson, JamesEG, JeLuF, Jec, Jemichel, Jhartmann, Jim.henderson, John a s, JohnOwens, JohnWittle, Johnblade, Johnnyboyshoots, Johnuniq, JonHarder, Joseph507357, Joyous!, Jtkiefer, Juanempere, Judzillah, Juliancolton, K45671, KGasso, Kakomo, Karagounis, Karn, Kasabas, Kate.woodcroft, Kb3rd, Khobino, Kbrose, Keith D, KelleyCook, Keraton, Kevmes, Kgfleischmann, Khalad, Kinema, King of Hearts, Kjolk, Knucmo2, Ksn, Kuru, Kvng, Kwanmikagami, Kwiki, Lamro, Laudaka, Lavenderbunny, Lee Carr, Leeb0, Leotholb, Lightmouse, Ligulem, LilaHelpa, Limbo, Limbo scrates, LittleBenW, LittleOldMe, Lockg, Lolpack, LordJumper, Lotu, Lovecz, Lped999, Lukith, Lumos3, Luna Santin, MER-C, MacGyverMagic, Mahojongg, Makeemlighter, Manish soni, Markjx, Martarius, Martijn Hoekstra, Matt.farina, Maury Markowitz, Mav, Mbutts, Melvinvon, Mendel, MessifCB, Mhare, Michael Hardy, Michael Sloane, Michael Thomas Sullivan, MightyWarrior, MightyM, Mike Rosoft, Mikm, Milan Kerslager, Mindmatrix, Minesweeper, Mnmszka, Modulatum, Mortense, MousePad, Moxyfire, Mozzerati, MrFish, MrOllie, Mrand, Mrh30, Mwanner, Myanv, N TRoPY, NJM, NawlinWiki, NeaNita, Nelson50, NewEnglandYankee, Nicolaasuni, Nighthraider0, Nikievich, Nishkd64, Nixdorf, Nhem, Norm, Northamerica1000, Now3d, Nroets, Nthep, Nubiatech, Nvj, Nynted, Oakad, Ohconfucius, Onhoitsjamie, Oneocean, OverlordQ, OwenX, Oxymoron83, Packetslinger, Palmer1973, Paul, Paul Koning, Peck123, Pekaje, Percy Snoodle, Peruvianillama, Petrb, Peyre, Pgallert, Pgan002, Phil Boswell, Philip Trueman, Piano non troppo, PierreAbbat, Pilatus, PinkMonkeys, Pjbrockmann, Pkirlin, Plasticup, Plugwash, Pluma, Pmsyyz, Praetor alpha, Prolog, Publicly Visible, QmunkE, Quarl, Quintote, RHaworth, RadioFan, Rait, Rapaporta, Ramy, Recurring dreams, RedWolf, Rednectar.chris, Reedy, Requestion, Rettetast, Rhobite, Rholton, Rich Farmbrough, RichardBennett, Rick Sidwell, Ricsi, Rjwilmis, Rlcantwell, RoySmith, Rrory, Roybadami, Royote, Rrror, Rsrikanth05, Rufus210, Ruud Koot, Rw4nd4, Rwww, SF007, SHCarter, Salsa Shark, Sam Hocevar, Sander123, Sceptre, Schneelocke, Scottf, SeaChanger, Selmo, Setu, Fisher, Shadowjaws, Shanes, Sharpard, Shieldforyoureys, Sietse Snel, Silenceisfoo, Sincoskie, Sligocki, SoSaysChappy, Sobelbob, SpamBilly, Spiritia, Steeve, Stephan Leeds, Stephemb, Steven Luo, Stratocracy, Stuart P. Bentley, Suruena, Svick, Swapdisk, Swarnabhra, TAnthony, Tas50, Tedernt, Template namespace initialisation script, Tempodivalse, Thaa00, The Anome, The Random Editor, The Thing That Should Not Be, The quark, The undertow, TheMoog, Thing2, Thue, TimBoeve, Tiny plastic Grey Knight, Tizio, Tmontval, TomPhil, Tonsofpes, Tooki, Tothwolf, Tpbroadbury, Transmission 1000, Trev M, Tunnie, Turgan, Tverbeek, Typ047, Tyz, UU, Ukepat, Ultric131, UncleBubba, Unschool, Uravbara, Useight, Utado, Vashti, Vdm, Veinor, Versus22, Vidmes, Vijaykumar, Viridae, Vmenkov, W Nowicki, Wa2ise, WadeSimMiser, Wasism, Wattlemsorse, Wavelength, Wayfarer, WaysToEscape, Wbenton, Wbm1058, Wefz, WhiteDragon, Wik, WikiJaZon, Wikiborg, Wikifranz, WillAndrews, WillLord, Willy on Wheels over Ethernet, Wimt, Wingnutamj, Wk muriithi, Wmahan, Wmasterj, Woohookitty, WriterHound, Wrs1864, Wtshymanski, Xenium, Xnatedawgx, Yintan, Yudiweb, Yuvalnod, Yyy, ZenerV, Zero10one, Zhangyue, Zodon, Zoiicon5, 1008 anonymous edits

**Link aggregation** *Source:* <http://en.wikipedia.org/w/index.php?oldid=508470483> *Contributors:* 2001:470:B01E:3:84BF:3A1C:388:D636, 7severn7, AdamJacobMuller, Aij, Al.locke, Arkrishna, Aryley, Ary29, Banec, Barcek, Beikarie, Binary.Side, Blatkinson, Brauhaus, Brianicus, C0nanPayne, Cadre, Cadvission, Chayashida, Cirt, CosineKitty, Cstizza1, Curtbeckmann, Cwolfsheep, DMahalko, DSToykov, Dalesc, Dkhydema, DragonHawk, Dthomson8, DeRahier, EagleOne, Eug, Fblancomo, Ffaye, Ffierling, Fiona-be, Fudoreaper, Geek2003, Googol plex, Guy Harris, H.scole, Hankwang, IMC Networks, IPSOS, Iamxsj, Intgr, JPG-GR, Jengell, Jmorgan, Joachim Schrod, Joscon5, Kagato, KelleyCook, Keitiltrout, Kvng, Lightmouse, LittleBenW, Lovinglolo, Lstricevic, MLD7865 Auto, Mandarax, Marce lito, Mark Bergsma, MathsPoetry, Maximus06, Mclean007, MrFish, Nealc, Notrehtad, Nuno Tavares, Nv8200p, Outlook, Pagingmrherman, PassportDude, PassportDude-1, Patrick Lucas, Pcrooker, Pelago, Petrb, Petri Krohn, Plugwash, PolarYukon, Puffin, Quadell, Sam Hocevar, Senthilk7, Stimson, The Thing That Should Not Be, Thumperward, Timaru, Tonkie, TonyHagale, Trixtor, Ttaglicht, Underpants, Vaya, Violetriga, Voidxor, Webhat, Weyes, Winterst, Wrelwser43, Xipher, Ybk33, 195 anonymous edits

**Power over Ethernet** *Source:* <http://en.wikipedia.org/w/index.php?oldid=507272682> *Contributors:* Adam Trogon, Adam850, Ali Thompson, Ali@gwc.org.uk, Antilived, Apanella, Armando, BW95, Bifter121, Bihco, Bilbo, Biot, Btilm, Cartque, Cheti, Coelacan, ColinATL, CommonsDelinker, Curtis Newton, Cyril.holweck, Danifel, Danl999, DavidCary, Dawnseeker2000, Dfallon, Dicklyon, Dkhydema, Dmbaty, Dobscure, Domaskuo, Doomed498, Download, Dpupkov, Dustinblack, ESkog, Echoray, Edward, Egolnik, Electron9, Eptalon, Eraserhead1, Erebus555, Evertw, Fgcsom, Fgnievinski, Flemirna, ForthOK, Fragglet, Gavron, Geek2003, Gene Nygaard, Giftlite, Glenn, Glrx, Gregmg, HenrikOlsen, IW4, Idleguy, Imroy, Indefatigable, Ironphoenix, Itusg15q4user, JLD, Javawizard, Jimz, Jnk, John Vandenberg, Karn, KelleyCook, Kvng, Lee Carr, Lmat, Lohray, MLD7865 Auto, Marcincak, Markus b, Mattgirling, Mboverload, Megya, Meros, Michaelkehoe, Mindmatrix, Miracle Pen, Mo aimm, Monedula, Morpheios Melas, Mr.moyal, Mtodorov 69, Muchness, Mugman, Nasa-verve, Neilc, Nelson50, Niceguyedc, Nicktaylor,

Niteowlneils, Nmarus, Ohados, Orpheus, PabloCastellano, Parkywiki, Pascal666, PassportDude, Pengo, Piast93, Piper8, Plugwash, Poccil, Pre-searcher, Requestion, Reswobslc, Rhobite, Rhombus, Ricci75, Rick Sidwell, Rjmunro, Rjwilmsi, Rspanton, Santosd, Splintax, Testbells, Texture, Tgwilsopedia, Thaas00, The Thing That Should Not Be, Thewalrus, Tholme, Tntdj, Tompw, Tonkie, Towel401, Trevj, UU, Usenymame3times, VSWR99, Vman049, Voidxor, W Nowicki, Wgcrafty, Woohookitty, Wtshymanski, Xchbla423, YUL89YYZ, Zodon, Zuxy, 287 anonymous edits

**Gigabit Ethernet** *Source:* <http://en.wikipedia.org/w/index.php?oldid=508613574> *Contributors:* Aldie, Alecv, AlistairMcMillan, Ametheus, Andrew sh, Aqualize, Aragon307, Armando, Asparagus, Atmchicago, Axilinx, Barrymyles, Bellhead, BenFrantzDale, Bernfarr, Bilbo1507, Bluewave, Bmcdonou, Bobblewik, Brewsum, Brian Gunderson, Briamski, Brupat, Cabling guy, Cate, Cburnett, Cbraschi, CharlesC, CloudNine, Cobigur, Crispnuncher, DavidBailey, Edward, Efa, Engineerism, ErandaXP, Esanchez7587, Evil genius, Excial, Extr transit, FT2, Flightsoftfancy, FlorianB, Fmcrown, Frap, Frodeaper, Gabbe, Giftlife, Glenn, Grasshopper, Guy Harris, Harland1, Henning Makholm, Heron, Hidden72, Hobart, Indefatigable, Intr, Jcole01, Jfromcanada, Jnanadev, Joy, KelleyCook, Kevin, KnightRider, Ktims, Kvng, Lee Carre, LeetHaxor, LucidGA, Markaci, Martarius, Mbemby, Mikeblas, Mild Bill Hiccup, MilongWong, Mkb218, Mrand, Nayakr, OLEnglish, Patcat88, Patrick0101, Philipp Kern, Phy1729, Pianoplayerontheroof, Plugwash, Pmsyz, Pol098, Radu - Eosif Mihailescu, Rbowman, Rchandra, Rdnetto, Reaper Eternal, RedWolf, Rednectar.chris, Requestion, Rfwatts, Rich Farmbrough, Robert.Harker, Sam8, Shattered, Shawnc, Slink pink, Spe01, Srleffler, StuffOfInterest, Sun Creator, Takteek, Tas50, Teles, The Anome, The emm, Thecheesykid, Thunderbird2, Tmtimon, UNHchabo, Veliath, Voidxor, W Nowicki, Woohookitty, Xnolanx, Yabbadab, Ykhwong, Zac67, 297 anonymous edits

**10 Gigabit Ethernet** *Source:* <http://en.wikipedia.org/w/index.php?oldid=497663883> *Contributors:* A. B., Aldie, Ali@gwc.org.uk, Andybryant, Annsilverthorn, Anrie Nord, Anthony Appleyard, Apyle, Armando, Austimurphy, Axilinx, Barek, Bentogoa, Bobblewik, Bobke, Bthetford, BusinessesTecho, Cavebear42, Cburnett, CecilWard, Chowbok, Christian75, CobbSalad, CommonsDelinker, Crissov, Crotalus horridus, Dale.cosgro, Daniel Luechtefeld, Danielieu, Darshana.jayasinghe, Datahead44, Dawnsseeker2000, Dc987, Delicates, Derekcassidy, DmitryKo, Drphilharmonic, Dwisser, E2550, Electron9, Ellery, Engineerism, FPisani, Foobaz, Frap, Fudoreaper, Gadfium, Ge10engr, Geek2003, Giftlite, Graham87, GregorB, Gurch, Guy Harris, HammondJr, Harej, Herberthuber, Heron, IKe, Indefatigable, Intr, JPG-GR, JSandbrook, JaGa, Jedmiller, JemicJ, Jfromcanada, Jkt, Jleighton17, JonHarder, Jonahorowitz, Kaneseu, KelleyCook, Kentoyama, Kevintolly, Kingdon, Klaus100, Knoll, Kvng, Kyriosity, LeiZhu, Lewellyn, Life of Riley, Lightmouse, LilHelpa, MER-C, MacFreek, Magioladitis, Mandara, Mark Bergsma, Martyvis, Matchmiller, MauriceTrainer, Mboverload, Mditto, MementoVivere, Mike Memmott, Mindmatrix, MitchellShnier, MrRadioGuy, Mrand, Nachoman-au, Nadia2008, Nick2fast, Nippoo, Npeers, Oshamsi, PassportDude, Patrick0101, Paul Foxworthy, Paul Koning, Pearle, Phy1729, Piano non troppo, Piper8, Plugwash, Plxtech1, Pnm, Quanstro, Quibik, R'n'B, Rahulmothiya, Rajaram, gurumurthy, Rchandra, Regex73, Rewoxoner, Rich Farmbrough, Rjwilmsi, Rkarlsba, Ron2, Roncarney, Sallyfiber, Sanfrannman59, Scottschweitzer, Shainer, Shariff07724, Silicon, Srleffler, StuffOfInterest, Suruena, Svick, T23c, Tlavel, Tejasnatu, Teuchter, The Anome, Thewalrus, Thingg, ThomasStrohmann, Thorwald, Todd Vierling, Twilsonb, UTF-8, UU, Ultra-Loser, Verdatum, Voltaire20198, W Nowicki, Webwat, West London Dweller, WikiReviewer.de, Woohookitty, Ysangkok, Zodon, Σ, おむこさん 志望, 371 anonymous edits

**100 Gigabit Ethernet** *Source:* <http://en.wikipedia.org/w/index.php?oldid=508779651> *Contributors:* A5b, Ales-76, Awardblvr, Bengt Larsson, BertK, Bomazi, Bp0, Brianski, Camil.matiska, CaryJW, Chowbok, Ckt2packet, CommonsDelinker, Csylico, DaveSchneider42, Davidya100, Dima373, DmitryKo, Duckbill, Entanglebit, FT2, Fudoreaper, Fulldescent, Gaius Cornelius, Geek2003, Giftlite, Gobonomo, Gsaru, Halilovic, Iglam, Isofox, J.delaney, Jasper Deng, Jeff Song, JoelRussell, John, JustAGal, KelleyCook, Kvng, Kwj2772, LiDaobing, Lightmouse, Lka, Lmatt, MattKitty, Maxsleg, Miiflyboy, Mindmatrix, Minna Sora no Shita, Mixabest, Mrand, Nw testing, Ohconfucius, Pmsyz, Quanstro, R'n'B, Rdprescott, RjilV, Rjwilmsi, Rudy88314, Sharuzzaman, Stephen Bain, Talitum, ThatWasThen, The Anome, Thebrid, Thewalrus, Thorwald, Thunderbritches, Tim1357, Twilsonb, Vvusiri, W Nowicki, Webwat, Xenanetworks, Zodon, 129 anonymous edits

**IP address** *Source:* <http://en.wikipedia.org/w/index.php?oldid=508461904> *Contributors:* \*drew, 09ialsharrai, 0waldo, 1.mallesh, 16@r, 1a2b3c4e5d, lexec1, 203.109.250.xxx, 20percent, 21655, 48states, 4twenty420, 5 albert square, 76df457hjkodfg, 7qlrl41r, 9258fahsflkh917fas, A Softer Answer, ABF, AVand, Abdul muqeet, Abecedare, Abmitgkp2011, Acalamari, Acather96, Accurizer, Acroterion, Adammw, AdjustShift, Aervanathan, AgainErick, Ageekgal, Agent007bond, Agentscott00, Agurzil, Ahkitj, Ahoersteimer, Ahly1, Airconsswitch, Airplaneman, Aitias, Ajuk, AlanRockefeller, Alanbrownie, Alansohn, Alex Cohn, Alex43223, Alison, AlistairMcMillan, Alpha 4615, Alphachimp, Alphax, AltecLansing12, Alvestrand, Amnuay, Andres, Andrewlp1991, Andrewski, Andy, Andy Dingley, Andy Smith, AngelOfSadness, Anna Lincoln, AnonGuy, Anonymous editor, Antandrus, AnthonyR, Anthonymetal, Apoyon, Applesqsx, Aqberr, Arakunem, Archer7, Argentium, ArglebargleIV, Arizona1983, Arman Cagle, Arthuran, Ashenai, Asoiaf fanatic, Atlani, AtomSmasher, Avnjay, Avogadro94, Avoided, Avono, AzaToth, Baccala@freesoft.org, Badmachine, Barek, BarretB, Bayberrylane, Benwildebor, Berro9, Beta m, Bethes1, Bfkolens, Bibroks, Bigjmr, Bihco, Bill37212, BioPupil, Bjankuloski06en, BlackAce48, Blake3522, Blanchardb, BlueCanary9999, Bluerasberry, Bluted, Bobblewik, Bobo192, Bogey97, Bongwarrior, Bovineone, Braaropolis, Brian0918, Brianporter, Brick Thrower, Brothejr, BryanG, Bubba hotep, Bubba73, Bubzyz, Bucketsof, BuickCenturyDriver, Bullzilla, CTZMSC3, Caltas, Can't sleep, clown will eat me, CanadianLinuxUser, Canaima, CannedLizard, Capricorn42, CaptainVindalo, Cardonnell, Cburnett, Cdc, CecilWard, Ceo, Cepopaladin, Cespar, Chacor, Chainz, Chamal N, Chaoobserver, Chase me ladies, I'm the Cavalry, Chasingol, Cherron1994, Chick Bowen, Cholmes75, Chopeen, Chris the speller, ChrisHodgesUK, Chriswiki, Chromaticity, Chuununa Baka, Chzz, CiTrusD, Cj005257-public, Cleared as filed, Cntras, Coasterlover1994, Cobi, Cometstyles, Comex, ConconJondor, Connormah, Controleoye, Conversion script, CorpX, Corti, Corvus cornix, Courcelles, Crazycomputers, Crazytales, Creative0o, Cremepuff222, Crystallina, Cst17, Cureden, Curps, Cwolfsheep, Cybjit, Cynicism addict, D-Katana, DARTH SIDIOUS 2, DJ Clayworth, DMahalko, DVD R W, DaL33T, Damicatz, Damore1405, Danhell666, Dandorid, Daniel Olsen, Daniel.Cardenas, Daniel15127, DanielCD, Danny, Dante20XX, Dark MooGoo, Darrell Greenwood, Darth Panda, David Levy, David.Mestel, Davidoff, Dawn Bard, Dcljr, Ddas, DeadEyeArrow, Deagle AP, Deannyc, Deman 24, Demmy, Denelson83, DerHexer, Darris, Digitalme, Dillard421, Dina, Diomidis Spinellis, Dionyviz, Discospinster, Dmafeti, Doc Daneeka, Doniago, Doria, Dougofborg, Doulos Christos, Dr.queso, Dragonball1986, Dragom flight, Dreadstar, Drkmaster, Drmies, Drunken Pirate, Drsprada, Dungodung, Dysepsion, Dzof, E0steven, ESkog, EagleOne, East718, Echuck215, Edward, Edward301, Egmontaz, El Monster, ElKevbo, Elassint, Elockid, Emersoni, Emo Elli, Emurphy42, Enviroboy, Eprb123, Er Kommandante, ErikVaalaa, Eric4, Escape Orbit, Eversac, Everything, Excial, Fagioloner, Falcon8765, Famspear, Faradayplank, Farquaadhchm, FastLizard4, Favonian, Fdgsdfgg rgfsgfd fdgsrfff, Feezo, FellowWikipedia, Ferrija1, Fieldday-sunday, Fleizach, Floaterfluss, Flyguy649, Forkazoo, Fox816, Fran McCrory, Francis22, FrancoGG, Frankie0607, Frap, Frazzyde, FreeKresge, FreelySpang, Freshmanicy, Friendly Neighbour, Fritzpoll, Frozenpandam, Funny Monkey, Furkyef, Fuzheado, Fuzzypieg, Fvasconcellos, Fvw, G.A.S, GICodeWarrior, GPugh, GT5162, Gadfium, GatI, Gaius Cornelius, Galoubet, Gamaliel, Gamera2, Gary99129, Gatlingunlevel27, GcSwRhlc, Geeoharee, Gengiskanhg, Geoffrey, George The Dragon, George2001hi, Gerardcohen, Giftlite, Gilliam, Glane23, Gnowor, Gogo Dodo, Golbez, Goldom, Gonzo fan2007, Goodnightmush, Graceful, Graciella, GraemeL, Graham87, Greswix, Grim23, Grunt, Guardians11, Guess9999, Gurch, Gurchzilla, Gwalla, Gwernol, H8erade, Haakon, Haei, Hadal, Hagerman, HalfShadow, Hall Monitor, Hansmohrid, HappyInGeneral, Haza-w, Hbackman, Heberkowitz, Hdt83, Henry W. Schmitt, Heracles31, HiDrNick, Hmxro, Hoijimachong, Home-4f8918a9a7\mshome, Hon-3s-T, Howabout1, Hughcharlesparker, Hughesey, Huskihuiskhusi, Hut 8.5, Huttar, Hydrargyrum, II MusLiM HyBRID II, IRP, Iancarter, Idcmp, Idts, Ilya, Immisslife, Immunize, Imperator3733, Imroy, Imveryveryverybored, InShanee, Indeterminate, Infrogmaton, Inspector 34, Intelati, Iorek85, Ipatrol, IraChesterton, Iridescent, Irishguy, IronGargoyle, Isseeaboar, Ixfd64, J-stan, J.delaney, J450NH3, JDoorjam, JForget, JHMM13, JLATondre, JR JakeRs, JTN, Ja 62, JaGa, Jackfork, Jackohake, Jackol, Jake Nelson, James ONeal, JamesAM, Jaredbelch, Jasper Deng, Jauerback, Jaxl, Jebba, Jeepday, Jeff G., Jeffrey Mall, JeremyA, Jesant13, JesseW, Jh51681, JidGom, Jj 37, Jkin, Inc, JoanThaBone, JoanneB, JoeKearney, Joeler31, John of Reading, John254, JohnWittle, Johndarlington, JohnnyB256, Johntheslade, Johnuniq, Jojhutton, JonHarder, JorgeGG, Josh Parris, JoshSkidmore, Jossi, Joyous!, Jpatokal, Jsalims80, Jsc83, Judik, Juliancolton, Junckerg, Junnel, Justafax, Jusjih, Jwissick, K12345wiki, KFP, Kafka Liz, Kaisershatter, Kanonkas, Kaplin, Karada, Karl-Henner, Katalaveno, Katieh5584, Kbndk71, Kbrose, Kelly Martin, Kesac, Kevin B12, Kevin66, KevinTjan, KgFleischmann, Khukri, King of Hearts, Kingjalis3, Kingpin13, Kinu, Kipoc, Kirill Lokshin, Kjd, Kjklon, Klepas, Klose99, KnowledgeOffSelf, Kookykman, Koolkat2448, Kraftlos, Krellis, Krunk, Kryptos, Ksn, Kthsujal, Kungming2, Kurku, Kurkyh, Kvng, Kwamikagami, Kwoksir, L'ecrivant, La Parka Your Car, La Pianista, LaMenta3, Labongo, Lam40, Lanasa, Latka, Law, Lawrence Cohen, LeaveSleaves, LegitimateAndEvenCompelling, Les boys, LibLord, Lightdarkness, Lilac Soul, Lilserif, LinguistAtLarge, Litefantastic, Little Mountain 5, LittleOldMe, LizardJr8, Lokimang, Lord Voldemort, Loren.wilton, Lostintherush, Lothar von Richthofen, Lotje, Lucinos, Luke wyatt, Luna Santin, Lupin, LyonJE, MER-C, MSSEVER, Mabuse, Mac, MacroDaemon, Maddiecke, Magister Mathematicae, Magnus Manske, Makeemlighter, Malcolm Farmer, Malhomen, Malo, Man1, ManiF, Manop, Marek69, Mark Renier, MarkSutton, Martarius, Martynas Patasius, Master Jay, Master of Puppets, Mastershake phd, Matthewrbowker, Matthuxtable, Mattiv2006, Maurog, MaverickSolutions, Maximillion Pegasus, Maxis ftw, Maxweb, McSly, Melonite, Melter, Mentifisto, Merovingian, Metaeducation, Met501, Michael Hardy, Michael Pheddyn, MikaeY, Mike Rosoft, Mindmatrix, Minna Sora no Shita, Mion, Mistorer, Mid zero, Mneerman, Mmernex, Mmmready, MonoAV, Montchav, Monty845, Moomoomoo, Moonriddengirl, Mormalig, Morning277, Mr.Z-man, MrJones, Mrsudip, Mschel, Mulad, Murderbike, Mushroom, Mwtowes, My Cat inn, Mygerardromance, Myihilihi, Myiptest, Myransree, Mrio, NSLE, Nagy, Naive cynic, Nakon, Nanshu, Nascar1996, Nastajus, Natalia, Erin, Nathamdotcom, NawlinWiki, Neeples, NewEnglandYankee, Newwhist, NickBush24, Nicklaus20, Nightscream, Nimew, Ninny777, Nishkid164, Niteowlneils, Nivix, Nlu, N123645, Nneonneo, No Guru, Noctibus, Nofallash, Nrlight, Nsaa, Nubiatech, Obakeneko, Ocateir, Odistry, OlmyΩ, Ohnoitsjamie, Oliver Lineham, OlivierMechani, OllieFury, Omicronperse8, OnePt618, OneCountry, Opelio, Orange Suede Sofa, OrangeDog, Orangutan, OrganizeFISH, Oshra schwartz, Ottawa4ever, OverlordQ, Oxymoron83, PRRfan, Pabix, Pachydermballet, Paddu, Pandion auk, Pantjz, PatchesTheCaveman, Patpink, Patrick, Patstuart, Paul Carpenter, Paul Magnussen, Paul Stanisfer, PaulHanson, PaulTinanenbaum, Pavel Vozenikel, PedroPVZ, Pepper, Perilwulruz, Persian Poet Gal, Peruvianflama, Peter, Peyre, Pg2114, Pharaoh of the Wizards, Photon87, Phrag, PhiKnight, Philip Trueman, Piano non troppo, PierreAbbat, Piet Delport, Pilotguy, PinchasC, Pinethicket, Pmlineditor, Pmsyz, Pnm, Poled, Ponies123456789, Poochy, PoochyPantsMcPooperson, PrestonH, Prolog, Pseudomonas, Psy guy, Puffin, Pyrop, Pyrosprout, Quintote, Quixuplusone, Qwyxrian, Qxz, RDaniel2, Rachtchi, Radiant chains, Radioactive afikomen, Rafasseb, RaiderTarheel, RainbowOfLight, Ralphwiggam75, Rameshbabu.itian, Rantsroamer, RattleMan, Razakausar, RazorICE, Rcaawsey, Rechandri, Remarot, Rdsmith4, Reconsider the static, RedHillian, RedWolf, Regancy42, RenRochefort, Rettetast, RevolverOcelotX, RexNL, Rfc1394, RiK harhar, Riana, Rianvisser, Ricgal, Rich Farmbrough, Richard001, Rjensen, Rjstott, Rlcantwell, Rmt2m, Rmstar 10, Robbie, Robby.is.on, Robocoder, RockMFR, Romanskolduns, Ronjhones, Rory096, RoyBoy, Rrburke, Rr, Rr, Rsm99833, RunOrDie, Ryamigo, Ryan032, Ryt, SEWilco, SG Bailey, Sahansuraeweera, Salamurai, Samilamethmal, Sango123, Santamage98, Sasquatch, Sayden, Scgtup, Schzmo, ScienceGolfFanatic, Sean D Martin, Sean.hoyland, Seanx820, Sebastian Goll, Sebleblanc, Sgarcia05, Shadowjams, Shadowlynk, Shanel, Shanes, Sherool, Shiftoften66, Shirik, Shirulashem, Shiva 29, Shoeofdeath, Shotwell, SidP, Sietse Snel, Sillicongal, Simetrical, Simon J Kissane, SimonP, Simonwhatley, Simple Bob, Sims2789, Simsong, SingingDragon, Sir Nicholas de Mimsy-Porpington, Sjakkalle, Sjö, Skier Dude, Skunkboy74, SlimVirgin, Slom02, SluggoOne, SmallPotatoes, Smileyrepublik, SmilingBoy, SoSaysChappy, Soliloquial, SonicAD, Soumyasch, Soundcomm, Spk, Spazit, Spazturtle, SpeedyGonsales, Spellcast, Spinningspark, Sportsfan 555, Spundun, SpuriousQ, SqueakBox, SquidSK, StabiloBoss, Stephan Leeds, StephenB, Supermon401, Superuserit, Supreme Deliciousness, Suruena, SusanLesch, Swalot, SymlynX, Synchrone, T3h 1337 b0y, TJ Spyke, TYelliot, Tangotango, Tannin, Tanthalas39, Tanweer Morshed, Tao, Taw, Tbhottch, Tcnv, Ted Longstaffe, Teh tennisman, Teles, Tgjotchi, The Anome, The High Fin Sperm Whale, The Return Of Squad, The Rogue Penguin, The Thing That Should Not Be, TheCoffee, TheGrimReaper NS, TheKMan, Thecosmos, Thegraham, Thekittenofterra, Thewayforward, Thingg, Threilafterthree, Thue, Tide rolls, TigerShark, Tim1988, Timpalthorpe, Titoxd, Tjwagner,

**Transmission Control Protocol** *Source:* <http://en.wikipedia.org/w/index.php?oldid=509454358> *Contributors:* 10metreh, 5 albert square, A-moll9, A1vast, A5b, Access Denied, Acdx, AgadaUrbanit, Agent Koopa, Agi896, Ahson7, Akamad, Akill, Akshaymathur156, Alca Isilon, Aldie, Ale2006, Alex, Alexescalona, Alexh19740110, Alexius08, Alt-sysrq, Alvin-cs, Amalthea, Andre Engels, Andy M. Wang, Anichandran.mca, Anna Lincoln, AnotherNitPicker, Anwar saadat, Aprice457, Arnavachaudhary, Arnhemher, Arsenal9boi, Asenine, Ashwinshbat, Astronomerren, Avono, Aw997, B4hand, BAxelrod, Banej, Beccus, Beland, Betterworld, Bezenek, Bigdumbuddinom, Bilbo1507, Bill Malloy, BillMcGonigle, Biot, Bkell, Bkkbrad, Blacksqr, Blanchardb, Booty443, Boscoscotti, Brech, Breno, Brighterorange, Brion VIBBER, Bstrand, Bubba hotep, Butros, C10191, Can't sleep, clown will eat me, CanadianLinuxUser, Canthusus, Cbrettin, Cburnett, Centrew, Charles.partellow, Chealer, Cheburashka, Christopher P, Cincaipatrín, Ciprian Dorin Craciun, Cjdanield, Clark-gr, CobbSalad, Coinchon, Colonies Chris, Cometstyles, Conversion script, Cpaasch, CRazH, CrizCraig, D25, DKEdwards, Daev, Daniel Staal, Daniel.Cardenas, Danielbarnabs, Danielgrad, DarriusT, DarkAudit, DaveSymonds, David.bar, Dcoetze, DeadEyeArrow, Dewet, Dgreen34, Dharmabum420, Dina, Djadawso, Dnas, DnetSvg, Doc Strange, Dori, DrHannibal216, Drake Redcrest, Duckbill, DylanW, Egg, Ego White Trav, Eirik (usurped), El pak, EncMstr, Encognito, Enjo4586, Enviroboy, Ebri123, Equentid, Eric-Wester, Erik Sandberg, Evice, Evil Monkey, Explicit, FDD, FGont, Fabiof, Fawcett5, Fcp999, Fishal, Fisherisland14, Flemira, Foobaz, Fred Bradstadt, Frederico1234, Fredrik, Fredrikh, Frencheigh, Fresheneesz, Fsiler, Fubar Obfuscous, Gaius Cornelius, GalaxiaGuy, Gamera2, Garion96, GarryAnderson, Ghettoblaster, Giffile, GilHamilton, Glenn Willen, Gmaran23, Gimaxwell, GoingBatty, Goplat, Graeme Bartlett, GrahamFountain, Graham87, Guy Harris, Gwinnadain, Haggis, Hairy Dude, Hamtechperson, Harp, HarrisonLi, Harryzilber, Harvester, Helix84, Henriktdborg, HiB2Bornot2B, Hilgerdenaar, I already forgot, I-balL, IOLJeff, IRP, Idcmpl, Ideoplex, Ititywybm, Imedcnl, Inroy, Inter, InTrg, Inwind, Izno, J. Nguyen, JCO312, JTN, Jaan513, Jackol, Jcarlos-causa, Jec, JeffClarkis, Jehorn, Jesant13, Jewbabca, Jfantsit, Jgeer, Jgrahn, Jjino, Jnc, JoanneB, Jogers, John Vandenberg, Johnnuniq, JonHarder, Jonathan Hall, Jondel, Jowagner, Jsavage, Jtk, Juliancolton, JuneGloom07, Jusdafax, Jxw13, Karada, Kartano, Karthick.s5, Kasperl, Katimawan2005, Kbrose, Kenyon, Kevininon, Kgflieischmann, Kim Bruning, Kinema, Klhuillier, Krellis, Kubanczyk, Kumarat9pm, Kyng, Kwamikagami, Kwiki, L Kensington, LachlanA, Lam Kin Keung, Lanilsson, Lark ascending, LeiZhu, LeoNomics, Leolaursen, Leszek Jańczuk, Leyo, LiDaobing, Lightdarkness, Lights, LilHelpful, Lilas Soul, Lime, Logiewax, Lokac443, Lone boatman, Longuninogirl, Loor39, Loukris, Ltampsros2, Lucasbf2, Luk, Luna Santin, Lunadesign, Lupo, M.S.K., MER-C, Mac, MacStep, Maclion, Maerk, Maimoi009, Makomk, Maksym.Yehorov, Mange01, Manlyjacques, Manop, Marek69, Mark Bergsma, Markrod, Martijn Hoekstra, Marty Pauley, Materialscientist, Mattabat, Mboverload, Mbruck, MeekMark, Meekohi, Mendel, Mhandley, Michael Frind, Michael Hardy, Mild Bill Hiccup, Miss Saff, MithrasPriest, Mjb, Mohitjoshi999, Mootros, MoreNet, Mortense, Mozzerati, Mr Echo, MrBoo, MrOllie, Mrzehak, MtB, MtSz, N328KF, NKarstens, Nateshwar kamlesh, Nave.notnihil, NawlinWiki, Nayuki, Nealcardin, Nedim.sh, NeiGoneWiki, Neo139, Neshom, Nestea Zem, Ngriffeh, Nifyk, Nikhil raskar, Nikola Smolenski, Niemiew, Nixdorf, Nk, Nneamerica1000, Nubiatche, Nviladkar, Ocaasi, Ojs, Okiemromoka (old), Oldiow, Oli Fith, Omnicronperse8, Ordoon, Ortinatore, Otets, Ouimetech, Oxacyanthous, Oxymoron83, P0per, PBSurf, PS3ninja, Padmini Gaur, Pak21, Palica, PanagosTheOther, Papadopa, PaulWay, Pde, PedroPVZ, Pegasus1138, Perfgeek, PeterB, Peytons, Pfalstad, Pg8p, Pgr94, Phandel, Phantomsteve, Phatom87, PhilKnight, Phuyal, Piano non troppo, Plainsong, Plugwash, Pluknet, Pmadrid, Poeloq, Prakash mit, Prasanmaad, Prashant.khodade, Prunk, PureRumble, Purplefeltangel, Putdstud, PXt, Quantumobserver, Quibik, Qutezue, RA0808, Raul654, Rdone, RedWolf, Rettetast, RevRagnarok, Revolus, Rick Sidwell, Rjwilmsi, Rodowen, RodrigoCruzzati, Rogper, RoyBoy, Rtclawson, Ru.in.au, Ryan Stone, SHIMONSHA, SWAdair, Saaga, SamSim, Samuel, Sasha Callahan, Savagejumpin, Sbnoble, Scienti, Scii100, Scorpiondianda, Scrool, Sdolini3, Sepper, Sergiode, Sethwim, Sh mana, Shaddack, Shadowjain, Shultz, Sietsje Snel, Sim, Sleight, Smappy, Smssarmad, Smyth, Snowolf, Some Wiki Editor, Spearhead, SpeedyGonsales, Splint9, Spoon!, Squidish, StephenHemminger, Stephenb, Stevenwagner, Stonesand, StradivariusTV, StubbyT, Suruena, Svinodh, SwisterTwister, Synchrite, Syp, THEN WHO WAS PHONE?, Talel Atias, TangentCube, Tariqabjoti, Tasc, Technobadger, TediumsFellow, Teles, Template namespace initialisation script, TfI, The Anome, The Monster, The Thing That Should Not Be, The-tenth-zdog, TheVoid, Tide rolls, Timotheus Canens, Timwi, Toh, Tomchiukc, Tommy2010, Torla142, Trou, Tuukkah, Umar4206, UncleBubba, Unixguy, Urmajest, Ursushorribilis, Uruiamme, Vedantm, Velella, Via strass, Vinu Padamanabhan, Vrenator, WLU, WikHead, WikiLaurent, Wint, Wkcheang, Wlgrin, WojPob, Wolfkeeper, Woohookitty, Wrs1864, Xaphnir, Ymiaji, Yonatan, Youpilot, Ysangkok, Yyy, Zachlipton, ZeroOne, Zeroboo, Zundark, Zvar, شات صوری, 1130 anonymous edits

**Internet Protocol** *Source:* <http://en.wikipedia.org/w/index.php?oldid=509029027> *Contributors:* 2w133, A-moll9, A. B., ARUNKUMAR P.R, Abb615, Abdull, Adagio Cantabile, Addihockey10, Aekton, Aggelos.Biboudis, Ahoerstemeier, Aldie, Altesys, Alvin-cs, Andareed, Andre Engels, Andywandy, Angelo.biboudis, Anon lynx, Antiuser, Anttin, Anwar saadat, Ardonik, Arkrishna, Attilios, BAxelrod, Badaneda, Bdeshman, Beefman, Benor, Bentogoa, Biot, Bjornwiren, Blanchard, Blehfu, Blue520, Bobo192, Borislav, Brest, Brianga, Bridgecross, Brim, Brohua, Bryan Dersken, Bryanbuang1993, CALR, Caltech, Camilo Sanchez, Capricorn42, Carandir, Carlo.Ierna, Casey Abell, Cbordset, Cburnett, Cydon37, Ceo, CesarB, Chealer, Chenzw, Christian List, Closedmouth, Conversion script, Coolcaesar, Coralmizu, Corruptcopper, Courcelles, Cverska, Cwolfsheep, Cybercobra, Cyclonenim, Cynthia Rhoads, DARTH SIDIOUS 2, Dan D. Ric, Daniel Staal, Daniel.Cardenas, DanielCD, DeadEyeArrow, Defyant, Demian12358, Denisarona, Dgw, Dmafei, Dnas, Doria, DrBag, Drugonot, Ducknish, Dwheeler, EagleOne, Echuck215, Eclipsed, Eequor, El Ci. Elfgyor, Enjoi4586, Epbr123, Erodium, EverGreg, Evil saltine, FGont, Felipe1982, Ferkelparade, Fish147, Florentino flor, Formulax, Forton, Fredrik, FrummerThanThou, Fa, Galoubet, Gamera2, Gareth Griffith-Jones, GaryW, General Wesc, Giftfile, Glane23, Glenn, Goatbutly, Graciela, Grafen, Graham87, Granbarreman, GreenRoot, Hairy Dude, Hardyplants, Harvester, Hayabusu future, Helix84, Hemanshu, Heter, Hughcharlesparker, I am Me true, IRedRat, Imaregina, Imcdnlz, Imroy, Intgr, Ixfd64, J.delanoy, JHolman, JTN, Jack Phoenix, Jadounrullah, JamesBWatson, Jarble, Jasper Deng, Jauhenij, JavierMC, Jdforrester, Jedsuryusa, Jeff Carr, Jheiv, Jiddisch, Jimgeorge, Jimys salonika, Inc, Jno, JohnGranNineTiles, JonHarder, Justsee, KD5TVI, Karl McLendon, Karol Langner, Katalaveno, Kbrose, Kgflieschmann, Kim Bruning, Kocic, Krellis, Kubigula, Kukini, Kvng, L Kensington, Latitudinarian, Liangent, Limitmagici, Lion789, Looxix, Lotje, Love manjeet kumar singh, Maerk, Mahabub398, Maitloom, Mamadd2002, Mange01, Manop, ManuelGR, Markr123, Marr75, Max Naylor, Melter, Mike Rosoft, Mikieminnam, Mindmatrix, Mion, NGNWiki, Naive cynic, Nakon, NawlinWiki, NeoNorm, Nialldawson, Nightraider0, Nimiew, Nixdorf, Noformation, Noldoaran, Northamerica1000, Nubcake, Nubiatech, Nugzthepirate, O, Ogress, Olathe, Otolemur crassicaudatus, Oxymoron83, Paolopal, Patrick, Paul, PaulHanson, PedroPVZ, Phatom87, Philip Trueman, Pinkadelica, Piotrus, Plustgarten, Poeloq, Poweroid, Ppcmailley, Python eggs, Rabbit67890, Recognition, Reedy, Reub2000, Rcgleg, Rich Farmbrough, Richard Ye, Rjgodoy, Rkrkorian, RobertG, Robocoder, Rsduhame, Ryamigo, Ryannmedaniel, Sandstein, SasiSasti, Scientizzle, Scientus, Scopereccep, Senator2029, Shiftoten66, Shlomiz, Shoeofdeath, Sir Arthur Williams, Sjaak, SkyLined, SmilingBoy, Smyth, Some jerk on the Internet, Sonix059, Sophie Bie, SpaceRocket, SpeedyGonsales, Sperxios, Stephenb, Stevey7788, Supalex, Suruna, Sysiphe, THEN WHO WAS PHONE?, TakuyaMurata, Tarquin, Teles, Template namespace initialisation script, Tezdog, The Anome, The Transhumanist (AWB), Thorpe, Timwi, Tiuks, TkGy, Tobias Bergemann, Tommy2010, Torla42, Trevor MacInnis, Tristantech, TutterMouse, UncleBubba, Urvabara, V-ball, Varnav, Vary, Versageek, Versus22, VillemVillemVillem, Warren, Wayiran, Wayne Slam, WCourtney, Wereon, Where, Whitepaper, Wik, Wikibob, Wikisircharachelle, William Avery, Winston Chuen-Shih Yang, Wknight94, Woohooikit, Wrs1864, Wtmitchell, Yahoolian, Yamamoto Ichiro, Yausman, Yidisheviryd, Yyy, Zarcillo, Zundark, Zuzzuu, میکاٹ، شات، سانچے، تیکنگ، تیکنگ، 510 anonymous edits

**IPv4** Source: <http://en.wikipedia.org/w/index.php?oldid=508986382> Contributors: -Majestic-, A.R., Abdull, Acather96, Adrian.benko, AlephGamma, Alexkon, AlistairMcMillan, Althena, AndreasWittenstein, Andrewmc123, Andypar, Angela, ArglebargleIV, Arjayay, Armando, Axelriv, Barro, Barryd815, Begoon, Bmpcer, Borgx, Breno, Brest, Bro1960, Brouaha, C. A. Russell, CCFKreak2, CWii, Calwatch, Calinou1, CaribDigit, Carlo.arenas, Churnett, CecilWard, Cesbar, Chr D Heath, Chrishtron0423, Christian80, Cm115, Cmichael, Conversion script, Coredesat, Corti, Crashdom, Cwolfsheep, Cybith, Cynical, DARTH SIDIOUS 2, DBigXray, DH85868993, Dan6hll66, Daniel Staal, Daniel.Cardenas, Danielbarbawas, DataWraith, DavidDelaine, DenisKrivoshoev, Dmaftein, Dnas, Dotnus, DreamGuy, Dsearls, Duffman, Dungkral, Ed g2s, Ed.C, Ekspiulo, El C, Electron9, Enjoi4586, Erickbarch, ErikWarmelink, EvilSS, Exallium, Faco, Favonian, Floydpink, FormulaX, Fred Bradstadt, Fredrik, Fresheneesz, Gallando, Gehlers, General Wesc, Giftlife, Glrx, Graciella, Graham87, Graven69, Gthm159, Hairy Dude, Hberkowitz, ILike2BeAnonymous, IREDRat, Ilario, Imroy, Indrek, Ironholds, JTN, Jasper Dene, Jbergste, Jbhoon, JeroenMassar, Jesant13, Jgeer, Jk2q3jrkllse, Jnc, Joelly, Johnnyboyshoots, Johntheslade, Joseph Solis in Australia, Joshua, Jyperon, Jwdlonal, KaaL, KaeSo, Karada, Kasperl, Katieh5584, Kbrose, Kevin66, Kgfeischmann, KhrOnNs, Khlvalamde, Kickboy, Kiore, Kmwiki, Krellis, Kvng, Kwamikagami, Kyng, Leuqarte, Liface, Lightmouse, Lph, Lukeritchie, M.O.X, MECU, Magioladitis, Magnus.de, Maimai009, Mange01, Marcoscm, Markrod, Melnakeeb, Mewashere1, MichaelGoldsteyn, Milan Keršlager, Mindmatrix, Miss Saff, Mintrebuchet, Mochi, Mokgen, Molerat, Morten, Mushroom, Nathan Hamblen, Nealmcb, Neelix, NewEnglandYankee, Nii Einne, Noldoaran, Nutubiech, Ojw, Omniplex, Onceler, Opelio, Outback the koala, Parent5446, Parkamark, Paul, PaulHanson, Pengo, Peterhoneyman, Phantomdj, PhilipTruman, Phoenix314, Phorque, Piano non troppo, Pmj, Pratikaran, Presto8, Ptmc2112, Raanoa, Ranto, Rantsroamer, Rhllhong, Rchandra, RevRagnarok, RxNL, Rjwilmis, Robert Brockway, RoySmith, Rpwoodbu, Ruwolf, RxS, RyanWKeen, Sarafankit, Sejessey, Seaphoto, Shane kerr, Simon J Kissane, Sirmelle, SmilingBoy, Smurrayinchester, SpacemanSpiff, Spearhead, SpectatorRah, SpeedyGonsales, Stephan Leeds, StrangerInParadise, Suruena, Swellesley, Taestell, Teemuk, Tenretnieht, The Anome, The Thing That Should Not Be, TheGreyArea, Themonsterliga, Thnidu, Tide rolls, Toolnut, Tyler.szabo, UU, Ultimus, Undeference, Versus22, Visiting1, Vivio Testarossa, Vuktari, Wavelength, Winston Chuen-Shih Yang, Wolfsbane2k, Woohooikit, Wrs1864, Wyksztalicoch, XaverHagger, Xibe, Yann Lejeune, Yyy, Zanetu, Zetawoo, Zfr, ~~dem0n, 515, ↪~~ anonymous edits

**IPv4 address exhaustion** *Source:* <http://en.wikipedia.org/w/index.php?oldid=508781343> *Contributors:* 1exel1, AWeenieMan, AdamRoach, Adeade00, Adriatikus, Ahunt, Aitias, Alansohn, AlexiusHoratus, Allen4names, Amcedwards, Amossaphia, Andrew Hampe, AngoraFish, AnonMoos, Appraiser, Arcantril, Armando, Arthur Rubin, Atlan, Audunv, Barryll, Ben Ben, Bender235, BiT, Biblbroks, Bitrot, Bs266, C1ester, Calimo, Calvin 1998, CaribDigita, CecilWard, Chowbok, Chris the speller, Chronulator, Cwolfsheep, Cybercobra, Cybjit, D.i.L., DAnonymous1, Dandior, Danlev, DataWraith, Davehard, Davidhorman, Defyant, DerekMorr, DisillusionedBitterAndKnackered, Donfbread, Donovanhide, Download, DragonflySixtyseven, Drbug, Droob, Dtaylor1984, Duckbill, Eatmorehippo, Elomis, Entropa, Eraserhead1, Extra999, Ezemeey, FT2, Frap, Frozen Wind, Fryn, Fsiler, Furrykef, Fwpummings, Gforce20, Giflite, Gigacephalus, Glenn, Golbez, Graham87, Greenrd, GregorB, HarDNox, Hmains, Homerjay, Hydrox, Iceskash7, Ilario, Intelligentfool, Ipnaven, IvanPozdeev, IvanKesson, JCDenton2052, JasperDeng, Jeff G., JeffHos, Jeffrey Mall, Jmv2009, Joefromrando, John Broughton, John Millikin, John Vandenberg, John of Reading, JohnGrantNineTiles, Johnunq, Jojalozzo, Jpg, Julesd, KD5TVI, Karada, Kbrrose, Kenyon, Khaain, Khr0ns, Kjolkob, Kjoolone, Kvng, L Kensington, LFaraone, LOL, Lampak, Lazybeam, Lemuel, Leotohill, Lighthouse, LordLopkest, Lopkif, LordChamberlain, the Renowned, MacTire02, Majora4, Mamyles, Mandarax, Margin1522, Mark Renier, Matthew0028, Mercury543210, Mild Bill Hiccup, Mindmatrix, Mintrick, Mro, NameIsRon, Nasa-averse, Naveenzherian, Nickshanks, Noisai, NomoNest, Ocnn, Optimist on the run, Ori.livneh, Ovbwiki, Owendelong, PHenry, Pdedlong, Photon87, Piledhigherdeeper, Plugwash, Pmj, Pol098, Quicksilver, RHaworth, RapturHunter, Rchanda, Remberway, Rich Farmbrough, Riwulmsi, Roentgenium111, Rossenglass, Ryalware, Samphy, Kava, Scientius, ShatteredSlade,

Slbrown1963, Smallman12q, SmilingBoy, Smurrayinchester, Speculatrix, Standardfact, Steffdavies, Stephen J. Brooks, Steve2011, Strategist333, Stux, Suburbanslice, Suit, Superm401, Symplectic Map, Syp, TJRC, TYelliot, Teemu Leisti, Teemuk, Teles, Tenretnecht, Tfl, The Anome, The monkeyhate, Thparkth, Thue, Thumperward, Tonkie67, Tonyhain, Tonyhansen, Torsch, Tpbradbury, Tqbf, Turidoth, Two Bananas, Vasilii Faronov, Walter Görlich, Wavelength, Wavetossed, Woohookitty, Wrs1864, Xanzzibar, Zildgulf, Zr40, Пуканов Кирилл, 789 anonymous edits

**IPv6** Source: <http://en.wikipedia.org/w/index.php?oldid=509609057> Contributors: 09 F9 11 02 9D 74 E3 5B D8 41 56 C5 63 56 88 C0 - hack, 128.107.253.xxx, 2001:44B8:3178:E800:0:0:B000:B1E5, 2001:44B8:3178:E800:F5D0:5DED:E7AE:8192, 2001:470:890A:1:216:D4FF:FEED:DF4B, 2001:db8, 2345us, 2A00:F480:4:134:8CD0:DE64:F766:A6EC, 2A00:F480:4:2A1:E02E:59C3:B36D:DB51, 49oxen, A3 nm, AJR, Abune, Accountholder, AceJohnny, Adam Conover, Adamthewebman, Adoniscik, Aeluwash, Aeons, Agent0111, Ahoerstemeier, Aigarius, Ajbool, Akamad, Alainkaa, Alansohn, Aldie, AlephGamma, Alex43223, Alexander UA, Alexkon, Alexwcoington, AlistairMcMillan, Allanlw, Allens, Amigan, Amybjayaa, AnandKumria, Anastrophe, Andareed, Anders Feder, Andoni Stroe, Andrew4u, AndyTheGrump, Annesville, AnonMoos, Antonis Christofides, Arbitrary username, Arichnad, ArnoldReinhold, Artemgy, Arthur Rubin, Aschwiegmann, Ashley Y, Astronautics, Atakdouq, Autonf0, Avanu, Axelrv, Baa, Badcalculon, Badon, Balachanderk, Barri, Basza, Bbpn, Bdesham, Belamp, Beland, Benabik, Benandorsqueaks, Benbest, Bender235, Bentendo24, Beoba, Bertra g, Bgraabek, Big Brother 1984, BioTube, Blaynew, Blubber42, Bobblewick, Bobo192, Booty m, Borgx, Bornapilot, Bousqu, Bovineone, Brandmeister, Breno, Brianmaddox, BrokenSegue, Brownsteve, Bruce404, Bsv109, Bugfood, BurnDownBabylon, C.S.Abiresh, CKD, CKerri, CableCat, Cal-linuX, Calvin 1998, Cameltrader, Cananian, Cantrel, Cap'n Ressmmat, Capek, Cap'er13, CapitalR, Captkirk, Carlosguitar, Centrx, CesarB, Cesarlovera, Cgdallen, ChaosR, Charlier 94, Charu, Charwinger21, Chaser, Chbars, Chris73, ChrisErbach, Chrisinspfd, Cinnamondouche, ClamDip, Closedmouth, Cloudmonkey, Cmdrjameson, Cmsb705, Coaxial, Cobi, Cometstyles, ComputinChuck, Confuciou, Conversion script, Corso84, Crazycomputers, Crd Alameda, Credema, Crispmuncher, Crl620, Crwth, Cst17, Cwolfsheep, Cyan, Cybercobra, Cybijt, Cyp, DARTH SIDIOUS 2, DBooth, DMahalko, DNSStuff, Daev, DalZot, Dale Arnett, Dan100, Dandorid, Daniel Luechtefeld, Daniel.Cardenas, DanielDeGraaf, Darguz Parsilvan, Darxus, Das7002, DataMatrix, Dave6, David Gerard, Davidhorman, Dawnseeker2000, Deepedeoyle, Defyant, DerekMorr, Dglynch, Diannaad, Dickguertin, Dicklyon, Dispenser, Djcschaap, Dlابتور, Dlange13, Dnas, Dnevil, DocRin, Dolda2000, Don4of4, Donreed, Dontonyoureyores, DragonflySixtyseven, Drangon, Dreawig, Drewehasman, Droob, Dwandelt, Dwmalone, Dylan Lake, Dylan620, E94ml, EDUBLE, EEMIV, EdBever, EdC, EdoDodo, Edokter, Edward, Ehn, Ejumper, El C, Eldar, Emonk72, Endpoint, Enjoi4586, Enquire, Equazion, Eradt11, Ere, ErikHaugen, EthanL, EugeneZelenku, Euphrosyne, Evil Monkey, Extropian314, FGont, FT2, Falcon8765, Falcon9x5, Farncombe, FatalError, Feedmeccreal, Feureau, Fewaffles, Figz, Firealwaysworks, FlieGerFaUsTMe262, Fluffy 543, Fnagaton, Folajimi, Foobar, Fragglet, Frap, Fredrik, Freeaqingime, Freshenees, Frnkblk, Fsterry, Gaius Cornelius, Galmicmi, Geekening, GerardM, Ghane, Giftlife, Giraffedata, Glanc23, Glen Hein, Glenn burdett, Glendavies, Glrx, Gimmaxwell, Gmedding, Gorffy, GovStuff, Graciella, Graham87, GrahamHardy, GreenReaper, Greg L, Gudeldar, Guiltyspark, Gunnala, Gurch, Gwernol, Gyrospsheru, HAI, Haakon, Hairy Dude, Haleya, Ham Pastrami, Hankwang, Hannes.nz, HarryHenryGebel, Hashar, Hatu7, Hawaiian717, Heberkowitz, Hdt83, Helix84, Hfastedge, Hires an editor, HobbesLeviathan, Holizz, Holmwood, HorsePunchKid, Hpa, Husky, Hvn0413, Hypersonic, II MusLiM HyBRID II, IRedRat, Ihope127, Ilja Lorek, Iluvcapra, Imarsman, Imroy, Imzogelmo, Incnis Mrsi, Incompetence, Infofarmer, Insanity Incarnate, Int21h, InterMa, Intgr, Intrepioin, Iromeister, IronGargoyle, Ironholds, Itojun, Ivolocy, J-D-Cronin, JI28, JHunterJ, JTN, Jaivovic, Jamesday, JameySharp, Jan1nad, Jansengius, Janto, Jerry1250, Jason Quinn, Jasper Deng, Jbossbar, Jclemens, Jddahl, Jec, Jeff G., Jeff02, JeffMorris, Jeffsw6, Jengelh, Jeremy Visser, JeroenMassar, Jfromcanada, Jhd, Jhwoodyatt, Jithrae, Jj137, Jnc, Jo3sampl, JodyB, JoeKearney, Joefromrandb, John Maynard Friedman, JohnOwens, Johnsmit4092, Johnnunji, JonDePlume, Jondel, Jonker, Jordandanford, Jordiapalet, Joshua Scott, Jtg, Julesd, Justjohn45, K0rana, KDS4444, Kaldari, Karada, Kasperd, Kattmannia, Kaypoh, Kb966k, Kbolina, Kbrose, Kcordina, Keilana, KelleyCook, Kenyon, Kestasjk, Kgfeischmann, Kieff, Kinema, Klaver, Koaf, Konikofi, Kozuch, KrakatoaKatic, Krellis, Kromeage, Kitomas8, Kusima, Kvaks, Kvng, Kynan, LP-mn, LUUSAP, LVNXN12, Lagesag, KHM, Latifladid, Laug, Lawrence Kong, Lightbulbcole, Likestheaction, Logan, Lord Chamberlain, the Renowned, Lotje, Lotu, Lousyd, Luigiacruz, M. B., Jr., M.O.X. M00dawg, Maalaoui, Macrakis, Madalibi, Madhav208, Madman91, Maduskis, Magioladitis, Mahtin, Maian, Majordragon, Manankanchu, Mange01, Mansoor.riz, Marcod'ltri, Marius p, Mark Bergsma, MarkMLI, Markus Kuhn, MarkusWanner, Martarius, Martyvis, Marudubshinki, Matchups, Mathboy965, MaxWilder, Maxim Masiutin, Mdd4696, Meand, Megan at ARIN, Melongrower, Meneth, Mentifisto, Mhd.ashraf, Michael B. Trausch, Michael miceli, Michael davie, MichaelBillington, Michaelgray2w, Midnightcomm, MihaOrela, Mike Rosoft, Mike Schwartz, MikeWren, Mikeyman12345, Mikrn, Mindmatrix, Minghong, Minimac, Mintleaf, Mitar, MithrasPriest, Mnmx, Mnudelman, Mobus, Molerat, Money23, Mordomo, Mormonsareloser, Mr Minchin, MrOllie, Mro, Msiebuhr, Muad, Mukkakukaku, Mulad, MureninC, N328KF, NYMets2000, Naclmud2032, Naff89, Nageh, NameIsRon, Napalm Llama, NapoliRoma, Narelle, Nasa-verve, Nashrul Hakiem, Nate Silva, Naveenpf, Nczempin, Nealmb, NerdBoy1392, NerdyScienceDude, Netrangerrr, Nhandler, Nicd, Ninjagecko, Nixdorf, Nineagle, No More TV, Noldoaran, Northgrove, Notbyworks, Nsaai, Nubiateg, Nurg, Nwbeeson, Nzseries1, OSborn, Od Mishehu, Ohnoitsjamie, Old Moonkar, Olipop, OlivierMehani, Oliwi, Omegatron, Omegium, Omicronperseit8, Omniplex, One half 3544, Onelinier, Orchistro, OriumX, Ost316, Ovideon, P.vishnu7, PabloStraub, Paine, Pankkake, Paolop, Paradox2, Paranoid, Parsmutaf, Pascal666, PassportDude, Pathoschild, Patrickdavidson, Paul1337, PaulHanson, PaulTanenbaum, Peak, PedroPVZ, Pejake, Pengo, Personman, PeterCScott, PeterKz, PeterStJohn, PhilHibbs, Philc 0780, Phoe6, Phoenix-forgotten, PierreAbbat, Pinkgothic, Pjrm, Planetsared, Plasticup, Plau, Pnm, Pointillist, Pontillo, Porttiki, Powerlord, Prabhulwki, Prolog, Prunesqualer, Psheld, Psz, Ptmc2112, Public Menace, Puchiko, PuerExMachine, Quaeostor23, Quantumobserver, Quebec99, Qwertysty, Qwertys, RHaworth, Raffen, Raghith, Rait, Ralphace, Random832, Rechandra, Reloran, Rd232, Rdenis, RedWolf, Redlazer, Relativitydrive, Rememberway, ReyBrujo, Reza 2638, Rgaushell, Rich Farmbrough, Richard W.M. Jones, RichIH, Rick Sidwell, RickBeton, Rilesman, Rischmueller, Roadrunner7, Robbie5006, Robert Brockway, Robomayhem, Rocketmen768, Ronz, Roy.wonder.cohen, RoyBoy, RoySmith, Rps, Rrius, Rwessel, Ryankearney, Rythie, Ryulong, Ryuzaki00, ST47, SWAdair, Sam Hocevar, Samantha of Cardyke, Sandeepsoman, Saran945, Sarutv, SaveTheRbtz, Scienti, Scj2315, Scot.somohano, Scottbadman, Scottywong, Scratchy, Sean01, Sebcastle, Segaa381, SelfStudyBuddy, Setherson, Sfan00 IMG, Sgeees, Shadowjams, ShakataGaNai, Shirishag75, Shultz IV, Sibi antony, Sick bug, Sigkill, SillyWilly, Simon J Kissane, Sirmelle, Sjmsteffan, Sjrosen, Skittles, Skybon, Slahrdzhe, Smallpond, Smarter1, SmilingBoy, Smurfl, Smurrayinchester, Snaxe920, Snory, Sobec, Socialservice, SolarWind, Some jerk on the Internet, Sonicus, Sosodan, South Bay, Southen, Spearhead, Spicemines, SpuriousQ, Squids and Chips, SrMico, Stefan, Stephan Leeds, Stephenb, SteveDavidsons, StuartBrady, Stux, Stwalkerster, Subsurfer, Sukenjain, Suruena, Suseno, Svick, SymlynX, Synchrone, Sysy, TJFV, TJRC, TYelliot, TarkMiche, Team4Technologies, Teapeat, Teemu Maki, Teemuk, Template namespacinitialisation script, Tenth Plague, Terilius, Terjepetersen, Tfl, ThG, The Anome, The Last Username I Could Think Of, The Nut, TheAnarcat, TheLight, Thean2000, Thehotelambush, Thehallowmaker, Thexchair, Thorpe, Thrindel, Thumperward, ThurnerRupert, Tim Capps, Titoxd, Tjh1234, Tmauer, Tmh, To Serve Man, Tommy2010, Towel401, Tpbradbury, Trejico, Trevor Johns, Tristanb, Trisweb, Trontonic, Trusilver, TwoHundredOk, Tyler, Ukh, Uncle Milt, UncleDoggie, UncleVinniy, Und1sk0, Unitacx, Universalcosmos, Uruiamme, Utility Knife, Vajrallan, Valenciano, Vanessa.beth, Vedantm, Vegaswikan, Verdy p, Veriodbg, Vertium, Vespristiano, Victor, Viniciustinti, Viperios, Visiting1, Voidxor, Voomoo, WJBscribe, Wahjava, Warren, WarthogDemon, Watain, Wavelength, WayneMokane, Weatherman1126, Weregerbil, Wetman, Weyes, Whatispcv6, Wiki13, Wikimoder, WikipedianYknOK, Wimt, Winston Chuen-Shih Yang, Wisco, Wk murithi, Wmahan, Wondertruck, Wrs1864, Ww, Woods, X-Fi6, Xandell, Xeltran, Xercses8, Xpclent, Yago, Yama, Yayay, Youssefsan, Yurik, Yuriviet, Zaclipton, Zaphraud, Zed5linuX, Zeerak88, Zemyla, Zenmohit, Zhackwyatt, Zmding, ZorphDark, Обдающий философ, 1683 anonymous edits

**Dynamic Host Configuration Protocol** Source: <http://en.wikipedia.org/w/index.php?oldid=509670578> Contributors: 78.26, 909078L, Abhayakara, Abhi3385, Abisys, Abune, Acroterion, AdamJudd, Adomiscik, Afiler, Aitias, Alanaris, Alansohn, Aldie, Alex rosenberg35, Alfio, Alison22, AlistairMcMillan, Allstarecho, Almightylinuxgod, Alphachimp, Alvin-cs, Amacucish, Ampsarus, Andareed, Andre Engels, Andrei Stroe, Animum, Anuragkr Gupta, Apokrif, Arichnad, Arkrishna, Ashakiran, Ashwin, Atomician, BL, BW, Bardo, BartRoos, BenAveling, Billdorr, Bobby D. DS., Bogdanjiusca, Bookbrad, BrianOfRugby, Brucefulton, CALR, Can't sleep, clown will eat me, Celarnor, Celinama, Centrx, CharlieEchoTango, Chealer, Chris 73, Chris the speller, Chrumps, ClanCC, Cleared as filed, Cliffb, Closedmouth, Coastalsteve984, Conversion script, Coutin, Ctmt, DARTH SIDIOUS 2, DKEdwards, DStoykov, DVdn, Danger, Daniel.Cardenas, Davee, Davidkazuhiro, Davidoff, Davidstraus, Dbu, DeadEyeArrow, Dee Jay Randall, Denelson83, Desiremore, Dgies, Dgw, DigitalSorceress, Dols, Dreadstar, Dremora, Dylan Lake, EagleOne, Earendur, Echosmoke, Edward, Egjose, Ehn, Electrified mocha chinchilla, Elwell, Enjoi4586, Enrique r25, ErikWarmelink, Evil Monkey, Ewlyahoocom, Feureau, Flash.killer, Fleung, Friday, FrostytheSnownoob, Fudoreaper, Furykef, G Sison, Gaius Cornelius, Gamera2, Gareth Owen, Gary King, Giftlite, Gimboid13, Grafen, Grenavir, Guru cool, Gwalker nz, Hackingyoundra, Hadal, Hanjiji, Hannes Hirzel, HarisM, Harsbhai, Hazphi, Hazzamon, Heberkowitz, Heathbar5477, Helix84, Hephaestos, Hide1713, Hughcharlespark, Hughey, Infofarmer, Ironywrit, IsUsername, JTN, JaGa, Jasoltape, JasonWoolf, Jasper Deng, Jimsv, Jobin RV, Jocinwip, Joerg Reisher, Josh Parris, Joy, Jrvz, Jude Rosario, Karora, Kartik Agaram, Kawanzaleroy, Kbrose, Kentyman, Kevinmon, Kgfeischmann, Kinema, King Toadsworth, Kingpin13, Kinu, Krellis, Ksn, Kubigula, Kurykh, Kvng, LAAFan, Labongo, Lacen, Lahiru k, Lightmouse, Lkinkade, Looxix, Loren.wilton, Lowellian, M4gnunom, M7, MER-C, Mahewa, Makeleeb, Man711, Mandarax, Mani1, Materialscientist, MattGiua, Matthuxtable, Maximbo, Mcgonrya, Mechanical digger, Memming, Michael Devore, Mike Dillon, Mike Rosoft, Mindmatrix, Ministry of Truth, Mking30, Moeron, Moondyne, Mr Stephen, MrExplosive, Msabramo, Mwtowes, NCdave, Nachmore, Nafmosaved, Nastajus, Naved 12, Netsnipe, Ngriffith, Nicticht, Nikai, Niemw, Nixdorf, Njboros, Nnp, Nubiathy, Nutster, Nv8200p, Ocker3, Ocram, Ojw, Omniplex, One, Ootachi, PCHS-NJROTC, PRBryson, PV=nRT, Publicosta, Pagingmrherman, Pandemic, Parag2010, Parbatyogesh, Paris.butterfield, PeaceNT, Pedant17, Peng, Phatom87, Philcha, Piet Delport, Pinkadelica, Pion, Pokemonmegaman, Prohlep, Pseudomonas, QRX, Quar, RJaguar3, Raano, Radiant chains, Raghav, RattleMan, Razimrant, Rchanda, RedWolf, Reub2000, Rfc1394, Rich Farmbrough, Richwales, Rikboven, Rjstott, Rjwilmsi, RI201, Rob Hoot, Rodrigo.haus, Roris, solaris, Rrburke, Rursus, SJP, Sam Korn, Sameer.sujeet, Savant83, Schae, Scott.somohano, ScottSteiner, Sdrtirs, Sessonmaru, Shady69, Shields020, Shiftoften66, Shiryae, Skyfiler, Slazenger, Snaruis, Spk, Spasemunki, SpeedyGonsales, SportWagon, Srbanator, Srbhanotti, Stephan Leeds, Stevenm.ict, Suburbanslice, Suffusion of Yellow, Sunray, Superborsuk, Superm401, Sureuna, Swatithorse, TYelliot, Taochen, Taoqirkhosa, Tcb, Teemuk, Tellyaddict, Template namespace initialisation script, Teraya, The Thing That Should Not Be, The.valiant.paladin, Theking17825, Thomas d stewart, Thumperward, Tide rolls, Tim.sylvester, Tothwolf, Toty3478, Tremilux, True Pagan Warrior, Trusilver, Tyler.szabo, Ummi, UncleBubba, Utcurts, VernoWhitney, Vijeshchandran, Vocaro, Waggers, Wasisnt, Wdrazo, Wereon, Wiki104, Wikisirracharlie, Wilson.canadian, Winter1, Wisco, Wisher, Wizzard2k, Wk murithi, Wrs1864, XLiquidIceX, Xhienne, Xionbox, Xoxon1kk1, Yesteraeon, YordanGeorgiev, Yuckfoo, Zac439, Zedla, ~demons, 915 anonymous edits

**Network address translation** Source: <http://en.wikipedia.org/w/index.php?oldid=509518117> Contributors: (, 65.29.90.xxx, Aapo Laitinen, Aawc, Aelantha, Aitias, Ajo Mama, Alan U, Kennington, Alansohn, Aldie, Alex Smotrov, Alex.atkins, Alex.zeffert, Alexhixon, AlistairMcMillan, Althena, Altrnr8r, Andrew Hampe, Andrewpmk, Andrewriddell2, Aneah, Angela, Ap, ArsénireDeGallium, Ashwin, Asymmetric, Balajisarathi, Barek, Bbpn, Benoit rigaut, Bevo, Bos-Herz edit acct, Brion VIBBER, Brynosaurus, Cate, Cbarby, Cburnett, CesarB, Cf. Hay, Cheung1303, Chowbok, Christian75, CommonsDelinker, Conversion script, Copsewood, Cotoco, Cpartenidis, Crazycomputers, Crispmuncher, CrucifiedChrist, CyberSkull, Cybijt, D235, DARTH SIDIOUS 2, Daf, Damienivan, DanielEng, Daveg1k, Daveofthenewcity, Dawnseeker2000, Dcoetzee, DevastatorIIC, Dgtisy, DiGiT, DisillusionedBitterAndKnackered, Droob, Drpixie, Drunzandspace2000, Dspradura, Dysprosia, EH74DK, Edcolins, Eddy264, Edward, Elssson, Eqwend1, Ergy, Everyking, Evil Monkey, Excirial, Felipe1982, Fenix\*NBK\*, Freshenees, Gandaliter, Gareth Owen, Gary King, Garyvdm, Giftlite, Giraffedata, Glenn, Goatassaur, Golbez, GorillaWarfare, Gracefool, Graham87, Grimmfarmer, Guiltyspark, Guitargod2323, Hairy Dude, HarlandQPitt, Harrymcogs, Heberkowitz, Helix84, Hovden, Hydrargyrum, Icarins, Imcdnzl, Indian, Iranway, Ivan Pozdeev, Ivan.Lt, J.delanoy, JHunterJ, JTN, Jan Kunder, Jasper Deng,

Jengelh, Jez9999, Jhbdel, JidGom, Johnuniq, Jokerspuppet, JonDePlume, JonHarder, Jondel, Jonshea, Josh Parris, Joshf, Joy, Jpbowne, Jsnx, Just Another Dan, Jyoti.mickey, KD5TVI, Karada, Karstbj, Kbdank71, Kbrose, Kenyon, Keycard, Kgfeischmann, Kristof vt, Ksn, Kvng, Kwi, Kzollman, Lavenderbunny, Leuk he, LiDaobing, Lightdarkness, LittleOldMe, LobStoR, Lspo99, M gol, MARQUIS111, MER-C, Magnus Manske, Mallow40, Maltest, Mandarax, Mannafredo, Manop, Marchash, MarcoTolo, Mav, Mditto, Melongrower, Mercury543210, Mindmatrix, Mintguy, Misza13, Mmmeg, Murjek, Mygerardromance, Naniwako, Nazli, Nealmcb, Nilmerg, Nimew, Nixdorf, Nkansahrexford, Nubiatech, Nurg, Nyttend, Oalbacha, Oystein, PPBlais, Para, Pash, Pde, Pdelong, Peyre, Photon78, Phemry, Philadams, Philbert2,71828, Piano non troppo, PierreAbbat, Pinkadelica, Plugwash, Pmsyyz, Pol098, Profchakraborty iitkampur, Psychocim, Quar!, Quest for Truth, Rabarberski, Ramsey585, Rchandria, RedWolf, Rick Sidwell, Robert Brockway, Rohithakral, Ross Fraser, Rrburke, Rushtoshankar, Ryan Roos, SF007, SLATE, SQL, SalineBrain, SaulPerdomo, Sbmehta, Seikkka Kaita, Shahid789, Shirimasesn, Shiro jdn, Sideswipe091976, Siipikarja, Simetrical, Simon South, SimonEast, SimonSellieh, Slackerhobo, Smalljim, SoWhy, Sollosonic, SpyMagician, Steelmans1980, Stephan Leeds, Stephenb, Steven Zhang, Sujirou, Sun Creator, Svetovid, Syndicate, Taestell, Tagishsimon, TakuyaMurata, Teles, The Anome, The Inedible Bulk, Tiddly Tom, Tide rolls, Tobias Bergemann, Tommy2010, TonyHagale, Tresiden, Tristamb, Truthanado, Tsunanet, Tverbeek, Twasono, Twilsonb, Ulric1313, UncleBubba, Urhixidur, Vanished user 5zariu3jisj04irj, VanishingUser, Wavelength, Wermher, Wiki alf, Wikipelli, Wimblykit, Winterheart, WithGLEE, WojPob, Wolf0403, Wolfkeeper, Wolfrock, Woohookitty, Wrs1864, Xnm0, Xpanzno, Yk4ever, YordanGeorgiev, Zap Rowsdower, Zhlmnc, Zondor, Zundark, 628 anonymous edits

**Simple Network Management Protocol** *Source:* <http://en.wikipedia.org/w/index.php?oldid=508963379> *Contributors:* A-moll9, A0209129, Awak3N, Aapo Laitinen, Abune, Acmeacme, Adonaicanez, Adzinok, AgentOren, Alansohn, Aldie, AlephGamma, Alexav8, Allens, Alvin-cs, Amlz, AnAj, Andre Engels, Andrei84, Andrew Hampe, Angela, Anrie Nord, Anwar saadat, Aozarov, Arleyl, Arthur Rubin, Attilios, Aylons, Banej, Bartjunkman, Behind The Wall Of Sleep, Beno1000, Billoindotnet, Bluezy, Boklm, Bollyjeff, Bovineone, Brookshaw, Cadvg, Cbdrorsett, Ccordray, Cdc, Chenzw, Chirag rajput, Chrisch, Chruck, Chuq, Cohesion, Cometstyles, Costello, Cp111, Cuñado, Cybercobra, Darkfight, Darren23, DaveKrieger, David Battle, Dead3y3, Dgtsyb, Dogcow, DoubleBlue, Dragonfire, X, Egorre, Ehevutov, Electriccatfish2, Emho, EncMstr, Endpoing, Enjoi4586, Ebpr123, Escape Orbit, EvanGrim, Florent Brisson, ForthOK, Fraggle, Fudgepenis, GPHemsley, Gardar Rurak, Ghettoblaster, Gogo Dodo, Grprince007, Grafen, HamburgerRadio, Hardaker, Hashar, Helix84, Hoverbloob, Hu12, Ifaqueer, Ilovenagpur, Imarksmit, JTN, Jetekus, Jim McKeeth, Jim1138, Jjarrett, Jnc, JonHarder, Jordan Brown, Joseaperce, Jpatokal, Jules3, Kbrose, Kgentryj, Kramesh, Knutux, Kokyun, Ksn, Ktdreyer, Kvng, Larry2342, LiDaobing, LimoWreck, Lkinkade, Lousyd, LukasRypl, Lukeritchie, Lzur, Maetrics, Maghnus, ManagementMan, Mancini, Mange01, ManuelGR, Maplebed, Marnues, Masirfan, Master Frog-o, Mateo2, Materialscientist, Matt Darby, Matthew V Ball, Mayank06, Mentifisto, Michael Hardy, Mindmatrix, Mojo-chan, MrOllie, Msjegan, Mwtwoes, Netdiva, Netsnipe, Nisan86, Nivix, Nixdorf, Nixeagle, Nizaros, Nnh, NotAnonymous0, Nubiatech, Oli Filth, Omniplex, Opello, Ouatic-2, Palica, Pedant17, PedroPVZ, Pete142, Pgilmian, Phatom87, PhilKnight, Pmendl, Pmooney, Postrach, Prunesqueler, R'n'B, Rakeshchella, RandomAct, Ray Dassen, RedWolf, Renatta njitwill, Rikboven, Rimtjoang, Rookkey, RoySmith, Russvdw, Ruud Koot, SAE1962, SBaker43, Schoff, Shadowjams, Sharewarepro, Sietse Snel, Sleske, Smdunmyer, Socialjest404, Some jerk on the Internet, Sonic1980, Ssircar, Stewartadcock, Stewartjohnson, Stijn Vermeeren, Storm Rider, Stormie, Suffusion of Yellow, Suruena, Swmed, Tabrez, Tellyaddict, Tenbase, The Anome, Thumperward, Tocharianne, Tree Biting Conspiracy, Trvh, USMstudent09, UU, UncleBubba, Uzume, Varnav, W1xiangzhuo, Wbenton, Wikichange7, William Wang, Wk murithi, Woohookitty, X00022027, Yaronf, Yhabibzai, YordanGeorgiev, Yurik, 661 anonymous edits

**Internet Protocol Suite** *Source:* <http://en.wikipedia.org/w/index.php?oldid=469772795> *Contributors:* 130.243.79.xxx, 203.109.250.xxx, 213.253.39.xxx, 66.169.238.xxx, A8UDI, Aapo Laitinen, Abdull, Abdullaiss04, Acceptus, Acertron, Aecon, Ahoeistermeier, Alansohn, Albano, Aldie, Ale2006, Alek Baka, AliMaghreb, Aliaspr, Alireza.usa, AlistairMcMillan, Amungale, Ana Couto, Aneah, Anna Lincoln, Anon lynx, Anorom, Arcenciel, ArchonMagnus, Arteille, ArticCynda, Avant Guard, Avicennias, Axcess, AxelBoldt, B4hand, Barberio, Barnacle157, Beland, Bender235, Bentogoa, Bernard Francois, Betterworld, Bezenek, Bhavin, Biot, Bloodshedder, Brimcomp, Branko, Breno, Brian.fsm, Brion VIBBER, Camw, Canthusus, CaptainVindalo, Carnildo, Casey Abell, Cate, Cburnett, Chaderhook, Cheesycom5, Ckatz, Clark42, Coasting, Conversion script, Coolcaesar, CrinklyCrunk, Ctm314, Cybercobra, Cynthia Rhoads, DARTH SIDIOUS2, Damiani, Yerrick, Daniel Staal, DanielCD, Darkhalfact, DavidDW, DavidDouthitt, Denisarona, DerekLaw, Dgtsyb, Dicklyon, Disavian, Dmeranda, Dnas, Dogcow, Donjrude, Doradus, Dorgan65, Doug Bell, Drphilharmonic, Duffman, EagleOne, Ed g2s, Edmilne, Edward, Edwardando, Eekester, Ekashap, Electron9, Ellywa, Elwood j blues, EnOreg, EncMstr, Enjoi4586, Ebpr123, Eptin, Equentil, EricL234, Erik Sandberg, Ethanthej, Etu, Evil Monkey, Evil saltine, Expensivehat, Falcon9x5, Falcor84, Ferkelparade, Fixman88, Fr34k, Freyr, GaelicWizard, Geneb1955, Gilliam, Glane23, Glenn, GlobalEdge 2010, Globemasterthree, Golbez, GordonMcKinney, Graham87, Gringo.ch, Gsl, Guy Harris, Haakon, Hadal, Hairy Dude, HarisM, Harryzilber, Hasty001, Hcberkowitz, Headbomb, Helix84, Here, Hoary, Holylampposts, Hpmpuyen83, Hyad, IMSOp, Ilario, Imednlz, Imran, Indeterminate, Indinkgo, Inhumandecency, Inomyabcs, Intgr, Itai, J.delanoy, JTN, Jackqu7, James Mohr, JamesWatson, Jantangring, Watkins, JesterXXV, Jimp, Jmdavid1789, Jnc, Joanjoic, John Vandenberg, Johnblade, Johnuniq, JonHarder, Joruna, Jrogern, Jsoon eu, Judafax, JustAGal, KYPark, Kaare, Kasperd, Katieh5584, Kbrose, Kim Birning, Kim Rubin, KnowledgeOfSelf, Kocio, Konman72, Koyaanis Qatsi, Krauss, Krellis, Kungming2, Kusma, Kvng, Kyng, Labongo, Larree, Law, Layer, Leapfrog314, Lee Carre, Locketine, Logitheo, Lova Falk, Luna Santin, Magioladitis, Magister Mathematicae, Maltest, Mandarax, Mange01, Manop, Marcika, Martyman, Martyvis, Master Conjurer, Matt Dunn, Mattbrundage, Matthew Woodcraft, Matusz, Mav, Mckoss, Mechanical digger, Meiskam, Mendel, Merlissimo, Metaclassing, Michael Hardy, Miles, MilesMi, Mintguy, Mothmolevna, Mrzaius, Mukkakaku, Mwarren us, Mzje, NMChico24, Nasz, Navedahmed123, NawlinWiki, Nealcardwell, Nealmcb, NewEnglandYankee, Ngriffeth, Nhorton, Nick C, Niteowneils, Nivix, Nixdorf, Nknight, Nmacu, Nobody Ent, Northamerica1000, Nubiatech, Nv8200p, Obradovic Goran, Oheckmann, Olathe, Otets, OttoTheFish, Oxwil, Oxymoron83, Palfrey, Papadopa, Patilravi1985, Paul, Paul Koning, Paulkramer, Perfectpasta, Peripitus, Pfalstad, Pharaoh of the Wizards, Phao, Piano non troppo, Pi0M, Plugwash, Pokeywiz, Posifit, Pps, Public Menace, Punjabi101, Putdst, Quinxorin, R'n'B, RaNo, Radagast83, Ramnath R Iyer, Rayward, Rbhaga0, Reaper Eternal, RedWolf, Reliablersources, RevRagnarok, Rich Farmbrough, Rich257, Richardwhiuk, Rick Block, Rick Sidwell, Rjd0060, Rjwilmsi, RobElby, RobertG, RobertL30, RobertF, Robot, Rodeosmurf, Ross Fraser, Rrelf, Rserpool, Runis57, Ruthherrin, SJIP, STHayden, SWAdair, Samjoopin, SasiSasi, Seaphoto, Sheldrake, Shii, Shiruna, Shiro jdn, Shizhao, Sietse Snel, Sitush, Sjakkalle, Skullketon, Smartse, Smjg, Snaxe920, SnoFox, Spmion, Stahla92, StanQuayle, Staszek Lem, Stefan Milosevski, Stephan Leeds, Stephenb, Suffusion of Yellow, Sully, Sunray, SuperWiki, Suruena, Svick, Swwhitehead, Swpb, Ta bu shi da ya, Tagishsimon, Tarquin, Techmonk, Techpro30, Template namespace initialisation script, TfI, That Guy, From That Show!, Thatguylift, The Anome, The Nut, TheOtherJesse, Theresa knott, Thingg, Thumperward, Thunderboltz, Thw1309, Tide rolls, Tim Watson, Timwi, TinaSDCE, Tmaufuer, Tmchz, Tobias Hoevekamp, TomPhil, Topbanana, Tr606, Tyler, Typhoon, Ukepxap, Unyoyega, Vanis314, Vegasawikin, Victor Liu, Violetriga, W163, Wadamja, Waggers, Wavelength, Werezgeek, West.andrew.g, Weylinp, Whereizben, Wiki104, Wikid77, Wikikrlsc, William Avery, Wimt, Winston Chuen-Shih Yang, Woolkeeper, Wonderstruck, Woohookitty, Wrs1864, XJamRastafire, Xeesh, Xojo, Xosé, Yakudza, Yas, Ydalal, Yudiweb, Yunshui, ZNott, Zac439, Zeerak88, Zfr, Zoiicon5, Zondor, Zundark, Zvezda111, ^demony, شات صوتی, 821 anonymous edits

**Internet Control Message Protocol** *Source:* <http://en.wikipedia.org/w/index.php?oldid=500556071> *Contributors:* Adamianash, Ajk91, Alerante, Alvin-cs, Andareed, Anggarda, ArielGold, Athaenara, B20180, Beowulf king, Bgraabek, BobHackett, Bradycardia, Caesura, Celtkin, Chealer, Conversion script, Courcelles, Dark knight, DeadEyeArrow, Dnevile, DrThompson, Drj, Electrocute, Enjoi4586, Face, Favonian, Fibrie, Forton, Fresheneesz, Fubar Olbfuso, Goeratic, Graham87, Grenavitar, Gwern, Hari36533, Hawaiian717, Huwr, J.delanoy, JTN, Jadhav.m, Jasminiek, Jay-Sebastos, Jengelh, Jnc, Joseanes, Kbroke, Kenyon, Kgfeischmann, Kinema, Kku, LAX, Mahboud, Mange01, Matusz, Mayonaise15, Meand, Mintleaf, Monkeymaker, Monkeyman, Mr link, Mremail1964, My76Strat, Naveenpf, Nimieu, Niteowneils, Nixdorf, Nuno Tavares, Omar35880, Osilkian, PeterB, Phatom87, Piper8, Plustgart, Pmsyyz, Pointy haired fellow, Polluks, Poweroid, Promethean, Quibik, Qwertys, RHaworth, Ranjiths, Rjgodoy, Romann, SarahEmm, Shellref, Sietse Snel, Sioux.cz, SixSix, Suruena, Template namespace initialisation script, The Anome, Tjipayne, Tobias Bergemann, Tstojano, Tuukkah, UncleBubba, Unixguy, Verdatum, VictorianMutant, Voidxor, Voomoo, Wayne Hardman, Whbstare, Wikisirracharie, William Avery, Woohookitty, Wrs1864, Xnm0, YordanGeorgiev, 227 anonymous edits

**Internet Group Management Protocol** *Source:* <http://en.wikipedia.org/w/index.php?oldid=499573670> *Contributors:* AS, Abolen, Accumulator one, AlephGamma, Antichrist, Apexprim8, B4hand, Bktoro, Cgcaster, Charles Matthews, DWay, David Newton, DeRahier, Ed g2s, Enjoi4586, Evan, Falcon8765, Grasshoppa, Grunzh, Gwalla, Hairy Dude, Harpreet82, Hede2000, Hoo man, JTN, Jandalhandler, Kaaal, Karada, Kbrose, Kenyon, Kgfeischmann, Kinema, Kvng, Leolaursen, Mange01, Mateo2, Metaclassing, Msiebuhr, Nictlich, Nikai, Nothing1212, Patrickdepinguin, Pchov, Pmlinero, Psu256, R. S. Shaw, R.srinivas, Raanoo, Rcronk, RedWolf, Robhu, Runkalicious, Ruwanindika, Salgueiro, Sango123, Suruena, SvartMan, Technobadger, Termininja, TheAMmollusc, Thumperward, Trasz, Wikihelp1, Woohookitty, Zoiicon5, Тиверополник, 123 anonymous edits

**Simple Mail Transfer Protocol** *Source:* <http://en.wikipedia.org/w/index.php?oldid=508866710> *Contributors:* 164.58.10.xxx, 1exec1, 2001:1620:F0A:1:EF7E:5240:353D:1F9A, 21655, Aapo Laitinen, Abdull, Adrian.benko, Aelfgiu, AhmedHan, Aitias, Alansohn, Aldie, Ale2006, AlistairMcMillan, Amatulic, AnK, Andareed, Andrew.cudzilo, Ans, Anwar saadat, Archwymr, Arvindn, Astrps, Augurr, Babbage, BabsiSnoeks, Bakulev, Barefootguru, Beland, Benefros, Beno1000, Bigdumbidnosa, Blueraspberry, Bonadea, Breno, Brianh, Brownb2, Bshurtz, Bunnyhop11, C777, Cafeduke, CecilWard, Cedders, Cedric db, Chbars, Chris the speller, Chrisahn, Christian List, ChristopherTStone, Cinedictum, Coneslayer, Conversion script, Corti, Cryptic C62, Cwlfsheep, DStoykov, Dave-ros, Dawnseeker2000, DerHexer, Devrishighosh, Diego Grez, DirkTheDaring, Dirkb8, EQual, Ebradshta, Edgarde, ElBenevolente, ElmIndreda, Elvey, Enjoi4586, Ebpr123, Equentil, Erdal Ronahi, ErikWarmelink, Excirial, FIL123456789, Felixkasza, Fences and windows, Flemirra, Fredhoysted, Fredrik, Free Bear, Frnkstn, GBL, Gargaj, Ghettoblaster, Gianfranco, GoingBaty, Graylorde, Grin, Gscsbohy, Hac13, Han Dang Quang, Hairy Dude, Hariva, HenryLi, Hirzel, Htaccess, Htonl, Hymek, IRbaboon, Janeiloart, Incni, Mrsi, Intgr, Ivolucien, JTN, JVz, Jake Wartenberg, Jasper Deng, Jhawk2k, Jim1138, Jlauria, Jleefde, Jmvbox80, JohnSmith, Johnuniq, Jonik, Joy, Julie Deanna, Kbrose, Kelly Martin, Kentuko, Kerberos976, Kinema, Krellis, Kuru, L Kensington, Lalala2005, Lapsus Linguae, Ljadata, Ldorflman, Leif, LeoNomis, Liangent, Lotje, MER-C, MKoltnow, MRLC94, Mabdul, Macquigg, Mange01, Marcus Qwertys, Mathiastck, Maxi, Mdmkolbe, Mentifisto, Message From Xenu, Michael Leeman, Milliped, Milomedes, Mindmatrix, Mordomo, Ms2ger, Mwtwoes, NTOx, Nabber00, Nacarlson, Nanshu, Napalm Llama, Nbarth, Neiliucs, Nephenites, Nixdorf, Nrawat, Nubiatech, Ohnoitsjamie, Omegatron, Omniplex, Osias, Pagingmrherman, Parasitical, Phatom87, Planetary Chaos Redux, Plugwash, Pokemonblackds, Pol098, Pratyeka, Quadro, Rajeve1486, Reach Out to the Truth, Recognition, Rich Farmbrough, Richwales, Rick Block, Rory O'Kane, Rxwxrxwx, SJFriedl, Samitalways4u, Samuel, Sceptre, Scipius, Scurless, Sdfisher, Sdtirs, Seffer, Shep68, Shlomif, Simsve, Sjmsteffan, Southpaw018, Speight, Squire55, Sshoe, Staffwaterboy, StaticGull, Stephan Leeds, Stormie, Suruena, TGDA, Tedp, Template namespace initialisation script, The Anome, TheKMan, Theopolisime, Thumperward, TkGy, Trusilver, Twocs, UBJ 43X, UncleBubba, Uriuammie, Usien6, Varantes, Versageek, VictorianMutant, Vlhsp, Washburnmav, Wilinckx, Will Beback Auto, WintersChild, Woohookitty, Wrs1864, Xbt, Xoder, Yahya Abdal-Aziz, Yaronf, Yiannis, Zac67, ZeroOne, Zondor, Zophelia, Тиверополник, 433 anonymous edits

**Internet Message Access Protocol** *Source:* <http://en.wikipedia.org/w/index.php?oldid=509778102> *Contributors:* \*drew, 13 of Diamonds, 217.126.156.xxx, ASk, Adam Marsh, Addshore, Ajh16, Alaniaris, Ale2006, AlexJTaylor, Alexcat, AlstairMcMillan, Allen Moore, Anclation, Android Mouse, Anirvan, AntonMravcek, Apollo11, Arteichi, Arjun024, Armando, Avisp, AzaToth, BabsiSnoeks, Barefootguru, Bdesham, Beestra, Beno1000, Billgordon1099, BobJohannessen, Brandonsturgeon, Caiafa, Chadlukes, Charlesrh, Chealer, Chrisahn, Christian List, Cmh294, Conversion script, Cosmoincarlow, Cwlfsheep, Cybercobra, DaleKiefling, Danejasper, Danitaz, Defrenrokorit, Deli nk, Doodledo, Drable, Draney13, Duplicity, EagleOne, El Cubano, Eliashc, Enjoi4586, Equentil, Eric-Wester, Erpingham, Ersalan, Espetkov, Estephan500, Excirial, Falcon Kirtaran, Faradayplank, FisherQueen, Fleminra, Frap, Fuzzygenius, Gardar

Rurak, Gary King, Gifflite, Gkanch, Glenn Anderson, Golem, Grafen, Guinness, Gwydion1, Gzbr, Hadrianheugh, Hairy Dude, HalifaxRage, Haseo9999, Hgd, Hhielscher, Hi878, Honta, Hyad, Imz, Intrigued-user, Ivan Pozdeev, J.delanoy, JTN, Jlang, Joanjoc, Joconnor, Johayek, Johnjosephbachir, JonHarder, Jonabbey, Jonik, Joseph Spiros, Julesd, Juliancolton, Kernesky, Kaszeta, Kbrose, Kedadi, Keegan, KneeLess, Koweja, Koyaanis Qatsi, Krellis, Ktinga, L.Petrik, Larrymcp, Lathspell, LeaveSleaves, LiDaobing, Liftarn, LobStoR, Mabdul, Mairi, Martin Kealey, Mboverload, Mcsee, Mdcougar, Mloughran, Moloch09, Mouse Nightshirt, Mr.Z-man, Mtwoews, Nagy, Natkeeran, NaturalBornKiller, Ned Scott, Nemec, NerdyNSK, Nestea Zen, Nixdorf, Nomeata, Nubiatech, Oceans and oceans, Oliphant, Omniplex, Omphaloscope, P00r, PeconicSky, Peyre, Pgk, Pgr94, Pit, Pmsyyz, Pol098, Popnose, R27182818, RG, Red Slash, RedWolf, Rich Farmbrough, Rick Block, Rjwilmsi, Ron Ritzman, Ronark, Rsforward, RussNelson, Rxwxrxwx, Ryochiji, SJP, Sakurina, Sciencewatcher, Sdfisher, Sdttrs, SidP, Sinan, Snori, Speedoflight, Squadri, StevenMcCoy, Suruna, SusanLesch, THEN WHO WAS PHONE?, Thoric, Thumperward, Tim Iverson, TimoSirainen, Timosa, Tkttravis, TravisHein, Trou, Ts4z, Tyler9xp, UncleBubba, Uthbrian, V.s.mousavi, Voidxor, WJetChao, Walling, Wcoole, Wik, WintersChild, Wrs1864, Wsheward, Yaronf, Yosri, Z4ns4tsu, Zac67, ZeroOne, Александър Цамутали, Петър Петров, 390 anonymous edits

**Lightweight Directory Access Protocol** Source: <http://en.wikipedia.org/w/index.php?oldid=438296663> Contributors: 0, 62.202.117.xxx, 62.253.64.xxx, A8UDI, AJackl, ANGELUS, Abeld, Ahoerstemeier, Alexbatko, Almightylinuxgod, Amillar, Amux, Andareed, Andrew Findlay, Anna Frodesiak, Anna Lincoln, Anon lynx, Aragorn2, Arcade, Arknascar44, Armando, Asciberras, Atstarr, Augustan, Avijit.ghosal, BabsiSnoeks, Bahar101, Bcwhite, Beland, Benjamin Barenblat, Bevo, BigSmoke, Brandon, Brene, Brevantes, CLKlunk, Cavrdg, Charles Brooking, Chealer, Chris Q, Christian75, Chuunen Baka, Combatentropy, Comestyles, Crkey, DGG, Dalesc, Danprits, Darrien, DavidHallett, Deflective, Demisarona, Dennette, DerHexer, Dewet, Diningphil, Dmsar, Doczilla, Dogcow, Dolda2000, DoubleBlue, DrRogla, Dustimagic, ESkog, EZio, EagleOne, E Poor, Edward, EmirA, Emmanuel JARRI, Emperorbma, Equentil, Exien, FF1959, Flewis, Folajimi, Fred Bradstadt, Gamma, Georgesawyer, GerardM, Ghettoblaster, Giraffedata, Gman124, Gpallis, Great Cthulhu, Grovejary, Grs1969, Gurch, HFuruset, Helon, Hhielscher, Highlandsun, Hotlorp, Hui2, IWWhisky, IanManka, Iridescence, IronJohnSr, Isnow, J-stan, J.delanoy, JTN, Jaanis2010, JakobVoss, Jaysrl, Jawavizard, Jay, Jbm212, Jdthood, Jeffschuler, Jiddisch, Joe Jarvis, JoeHenzi, Jonathan de Boyne Pollard, Joonga, Jordan Brown, Jordau, Juliank, Jwilleke, Jxn, Kbrose, Kdz, Khendon, Konman72, Kozuch, Kuru, Kvng, Kwamikagami, LCE1506, Lazki, LeeCarre, Lesterriera, Levin, Looxix, Los on belmont, Lotje, Lukegn, Lysdexia, MMSequeira, Magioladitis, Mallamace, Manavmohanty, Manishearth, Manser, Marc Esnouf, Marcus Qwertus, Marek69, MarkWahl, Marty.offe, Matt Crypto, Maximaximax, MilkMiruku, Mindmatrix, Monkbel, MooingLemur, Mortein, Mpelyo, Mr stupid, Mrbill, Nabber00, Neelkanthriptathi, Nick, Nippoo, OLEnglish, Omniplex, Oneiros, Oxymoron83, Pabix, Parputa, Pascal, Tesson, PatrikR, Pedant17, Peterblaise, Pgan002, Phatom87, Pieffe, Pte Delpot, Pit@0xx.at, Pnm, Polluks, Poor Yoric, Premil, Pxma, RFightmaster, RW Dutton, Rageear, Randy Johnston, Rasmus Faber, RedWolf, Redjar, Remi00, Renaissance, Rhubarb, Rick Block, Rnapiere, RodWiddowson, Ronabop, RossPatterson, Ruakh, Rwoodsmall, Ryan Vesey, S3000, SJK, Sadads, Saligron, Sam sun, Scratchy, SebastianBreiter, Shadow1, ShelfKeweld, Shshme, Smaines, SmartIcon, Sunpha, Southen, Srpnor, StaticGull, Stephan Leeds, Stevage, Stickee, Subversive.sound, TRS-80, Taw, Taxman, Tbird1965, Tedp, Tero, The Master of Mayhem, The undertow, Thingg, Thumperward, Tide rolls, Timotab, Tlesher, Tobias Bergemann, Tobias Hoevekamp, Tothwolf, Towo, Treydrake, Turnstep, Tyler.szabo, UncleBubba, Uselesswarrior, Vanished user 39948282, Varlaam, VictorAnyakin, Vitund, WRJ, Waddey, Wageslave, WBenton, Wereon, Wiki alf, Wilsonhughes, Winterst, Wk muriithi, Woohookitty, Wsheward, Yingyang, ZZyXx, 641 anonymous edits

**Routing** Source: <http://en.wikipedia.org/w/index.php?oldid=509772324> Contributors: 16@r, 212.150.1.xxx, 777sms, Abdi1543, Adamianash, Aegicen, Afroenerator, AgentPeppermint, Akc9000, Aldie, AlistairMcMillan, Altemann, Alvestrand, Anna Lincoln, Arthena, Arunrkaushik, Ansanj, Azrael81, Azuris, Bacala@freesoft.org, Bjankuloski06en, Black swallow, Borgx, Brest, Brewhaha@edmc.net, Bruce lee, Bryan Derksen, Brynosaurus, Callmejosh, ChooseAnother, Chrescht, Cioto, Cojoco, Conversion script, CosineKitty, Cybercobra, D. Recorder, DRAGON BOOSTER, DSRH, Darth Panda, David Lundberg, DavidLevinson, Delaszk, Dgtsyb, Dominic, Dpahlk, Durty1425, Easylife12c, Echoray, Elf guy, Emperorbma, EvanGrim, Everything, Extraordinary, GentooBox, Gifflite, Gilliam, Gioto, GoingBatty, Good Olfactory, Graldensblud, HRV, Haakon, Iceflight, Imdcnld, Informedbanker, Insanity Incarnate, Isidore, Isnow, Itai, JTN, JaGa, Jacob grace, Jadams76, Jec, Jeltz, Jflabourdette, Jim1138, Jnc, Jelldopips, John lindgren, Joseph Dwayne, Joy, Junckblocker, Jwestbrook, Kablammo, Kanags, Karthikkte, Kbrose, Kdinesh, Khattab01, Kjkolb, Kozuch, Kremsko, Kvng, Lifefeed, Lilac Soul, LuciusAgrippa, M.dueli, M2petite, MER-C, MLD7865 Auto, Maury Markowitz, McBride, Michael Angelkovich, Michael Hardy, Mindmatrix, Minesweeper, Miseriou, Mmernex, Mmmeg, MrNerdHair, Mwalsh34, N328KF, Nealmc, NeoJustin, Nethgir, Neverquick, Nikosdimos, Nmacu, Ocker3, Omarecd, Orange Suede Sofa, Orrc, Oxymoron83, Paul, Pdelong, Pedant17, PGallert, Phatom87, Phil Christs, Phyzome, PierreAbb, Piet Delpot, Powo, Princessmarisa, QueenCake, Quidam65, Qwe, R3m0t, Rebounder, Red Thrush, Redsel, Rick Sidwell, RickK, Sevas, Shahid789, Shrads1984, Sonett72, SpaceFlight89, Stephenb, Stevenmitchell, Stl, Takanoha, Taxman, Tecman, Thanhtanbor, That Guy, From That Show!, The Anome, Thijswijs, Tide rolls, Tjwagner, Tobias Bergemann, Todd Vierling, Towel401, Tregoweth, TripleF, Tristamb, Umreemala, Una Smith, UncleBubba, Unreasonabledude, Unyoyega, Uriah923, Vary, Vineetkrjoshi, Vipulvyas, Visor, Wadamja, WBenton, Weregerbil, Wernher, West London Dweller, Weyes, Whocouldibe5, WikHead, Wmahan, Wolfkeeper, Woohookitty, Wrc60, YUL89YYZ, Yama, YordanGeorgiev, Youandme, Youssefsan, ZabMilenko, Zahnradzacken, Zoobee79, 342 anonymous edits

**Static routing** Source: <http://en.wikipedia.org/w/index.php?oldid=500638196> Contributors: Ackepenek, Afil, Bruno Santeramo, Butt.usmanali, CL, John 34345, MER-C, Mattsw, Omicronpersei8, Pgallert, Qwe, Rozbilen, Smalljim, Terrys01, VipX1, Woohookitty, Yhabibzai, 58 anonymous edits

**Link-state routing protocol** Source: <http://en.wikipedia.org/w/index.php?oldid=502499368> Contributors: ABSOLUTAMENTE, Aleksey Gerasimov, Alvestrand, Bilbo1507, CambridgeBayWeather, Chris Roy, Chris the speller, Chrisjameskirkham, Devaki.vamsi, DonaldEastlake3, Dudesleeper, Dummor, Ejrh, Emdad87, Gamera2, Garosenb, Geek2003, Hoju, Itai, Jackfork, Jaw959, Jnc, Joel.Conover, Jon Awbrey, Karn, Kbrose, Ketil3, Konstable, Lingathoor, MC10, Naddy, Nbeckman, Nethgirb, Nicgeuyede, Nixdorf, Omarecd, Pdelong, PhilKnight, Philip Trueman, Pmari, QEDquid, Random contributor, RedWolf, Roeme, Rönin, Scytale.de, Spookycafe, Tangotango, Thesavagenorwegian, Timo Laine, User2004, Vdham, Victor--H, Vyzasaty, WBenton, Woohookitty, 141 anonymous edits

**Open Shortest Path First** Source: <http://en.wikipedia.org/w/index.php?oldid=509724201> Contributors: A Meteorite, ALargeElk, Agreehalgh, Aldie, Alexf, Alisterb, Allens, Andrei Stroe, Andyluciano, Anon lynx, Antonvanderleun, Anuragkothari, Ari.takanen, Astralblue, Attilabedo, Avto.prangulashvili, AxelBoldt, Babinos30, Biot, Blaxthos, Bomazi, Bradleyem, Breakingaway, Brianga, C46, Can't sleep, clown will eat me, Caruch6392, Catamorphism, Celinama, Chealer, Cwolfsheep, Dandorid, Darthsco, Deineka, Dgtsyb, Dicklyon, Dinomite, Dougluce, Dysprosia, EJSawyer, Enjoi4586, Evan2008, Foobarnix, Franboop, Fudoreaper, Gifflite, H8a1r1819, Hads1, Hangin10, Hashar, Heberkowitz, Hede2000, Hilmarz, Hns, IMSO, Iamregin, Ibc111, Insanity Incarnate, JHunterJ, JTN, Jac16888, Jakub Horky, Janizary, Javifs, Jawpers, Jeffreyahnies, Jerome, Jialiango, Jkurnyj, Jnc, John, of Reading, Johnuniq, Jon Awbrey, JonHarder, Joy, JitToo, Kbrose, Kcley, Kenyon, Kinema, Kingpin13, Knowledge12109, Kozuch, Kryptimind, Lightmouse, Lineslarge, Lotje, Luc4, MARQUIS111, MarsRover, Materialscientist, Mbumber, McHildinger, MessiFCB, Michael Hardy, Mickdermack, Mlewiss000, MrOllie, Mwalsh34, Nate, Nbarth, Nealmc, Niekk01, Niemivh, Ninjamaster8, Niteowlneils, Nixdorf, Nkansahreford, Nothingwater, Nubiatech, ObfuscatePenguin, Omarecd, Omicronpersei8, Onceler, Pairadox, Palthainon, Paluchpeter, Pankkake, Pchov, Pgallert, Phil Boswell, Phil Holmes, Pewiki, Radagast83, Rfc1394, Rick Sidwell, Rjwilmsi, Roshjack47, Rubiojo, Samriva, Seronline, Shahid789, Sigkill, Sigma 7, Skor, Snowoul, Souliviu, Spxrios, Sreeakshay, Sreya1102, Srleffler, Ssrao08, Stephan Leeds, Stork, Suruena, Svick, Takanoha, Taral, Teles, Testbells, TheGrimReaper NS, Thejanapesegeek, Tigaente, Tintin107, Tmauer, Toe Rag, Tomaxer, Uday, UncleBubba, Vdham, Vjardin, Wavelength, WBenton, WBenton-test, Wisden17, Wisq, Wk muriithi, Woohookitty, Wrcarm, Wtmitchell, Wtt, Xclient, Zamfi, Zr2d2, 458 anonymous edits

**Routing Information Protocol** Source: <http://en.wikipedia.org/w/index.php?oldid=508613411> Contributors: AS, Ahoerstemeier, Ahull, Akc9000, Alan.murray, Alansohn, Aldie, AlephGamma, Alexh19740110, Allolex, Andareed, Andre Engels, Anon lynx, Barberio, Bleflu, Borgx, CSW1986, Callidior, Cybjit, Dajp, DanCasas, Dansen926, David-Sarah Hopwood, Dgtsyb, Dinomite, Druiloor, Drunkenmonkey, Ducknish, Endobson, Enjoi4586, Epbr123, Fab, FlavioMartins, Gamera2, Georgette2, Gmalkin42, Goat-see, Gustavb, H2g2bob, Hadal, Hairy Dude, Heberkowitz, HeathPetersen, Helon, Honeyman, Iamring, Iridescent, JHunterJ, JTN, Jakew, Jec, Jnc, Jon Awbrey, Jwoodger, KDSTV1, Kbrose, Kotiwalo, L33th4x0rguy, Lachlancooper, Lamny68, Lightmouse, Lls71, Maffommie, Magioladitis, Mercury43210, Methosant, Mgeorge27, Michael j harris, Micmon, Minusf, Mnerman, Mnernex, MrOllie, Mureininc, NCurse, Nealmc, Neilec, Niimivh, Nixdorf, Nkansahreford, Northernhenge, Ohnoitsjamie, Oxymoron83, Paul, PaulVIF, Peripitus, Pgallert, Piet Delpot, Pmsyyz, Poor Yoric, Ps-cz, R.srinivasas, RJaguar3, Raju5134, RedWolf, Redlazer, ReinforcedReinforcements, Reisio, RexNL, Robert Brockway, Ronz, S.boginskis, Sdrtrs, Seth Nimbosa, Sfischer, Shadowjams, Shahid789, Simon.clayton, Sjc, Skandha101, Suruena, Takanoha, Termininja, ThFabba, ThaddeusB, The Anome, TheGreatFoo, TimonyCrickets, Tomek0001, UncleBubba, Vary, Vickeybhopal, Vjardin, Wisamzaqoot, Yaris678, Yashpundir, Zamfi, 268 anonymous edits

**IEEE 802.11** Source: <http://en.wikipedia.org/w/index.php?oldid=509444507> Contributors: 130.94.122.xxx, 16@r, 28bytes, 2mem, 802dot1ln, 802geek, AboutWeezer, Academic Challenger, Acrisip, Adrians, Afed, Ahoerstemeier, Ahull, Ajj, Ajhuang-wiki, Alarob, Alcksmtb, Algov, Alinor, Allstrak, Almamun, Alphax, Amaelzer, Anastrone, Andres, Andros 1337, AngryBear, Ankur, Anáron, Apoyon, Arendswinter, ArielGold, Armando, Armin76, ArnoldReinhold, Arrenthe, Arstebos, Asocall, Astronautics, Asunasun, Ausinha, Austin Hair, Avargasm, AxelBoldt, Ayudante, Barbjfox2000, Bbabul01, Bcorr, Beland, Bent00, Bibrydo, Biot, BishopNight, Bluemoose, Blueberries, BoKu, Bobblewik, Bobo192, Boobytrapped, Bpdlr, Briandjohnson, Brianski, Bsilverthorn, BurntBiscuits, CAPITALIdea, CWii, Callidior, Caltas, Castien, Catgut, Cburnett, Cdc, CecilWard, Cecilyen, Certz, Cfrost, Griffiths, Chiefcoolbreeze, Chomperhead, Chris181, Cimaran, CityOSilver, Ckujau, Cleared as filed, Coasterlover1994, Conversion script, Cowgod14, Cpl Syx, Crh0872, Crimson30, Crissov, Ctbolt, CyberSkull, Cybercobra, Cyrius, Dafocus, Dake, Dancter, Dane.brink, Danks14, DarwinE, David R. Ingham, DavidAndersen, Dawnseeker2000, Dbenbm, Ddxc, Defrector, Dejvid, Denisarona, DerHexer, Derek Ross, Dirkvdm, Discospinster, Dj245, Dig2006, Dobz116, DocWatson42, Docu, Dogcov, Dqeswn, Drewzhrodague, Drj87, Dsheffie, Dtwtowski, Dwheeler, Dzubint, Eadrie, EagerToddler39, EagleEye96, Eatrains, Edderso, Editor B, Edokter, Ehn, Elkman, Engineerism, Enjoi4586, Epbr123, Erencexor, Erylicy, Eth01, Europrobe, Everything, Evgeni Sergeev, Evilspoons, Excirial, ExportRadical, FF2010, Faramir 27, Fennec, Fernandopabon, Fijal, Flemirna, Fosmez, Frecklefoot, Freddydead, Fubar Obfusc, Fudoreaper, GCW50, GFellows, Gaelen S., Garth 187, Gauthier, Gavinito, Glebleem, Gene Nygaard, Geppy, GianlucaCiccarelli, Gifflite, Gilesmorant, Glennf, GoingBatty, Goodput, Gorkish, GraemeL, Graham87, Grayshi, Gutza, Guy Harris, Hairy Dude, Heegard, Hellisp, Hetai, Hoho, Hotdog41695, Hqb, Hrhssolei, Huru179, Hvn0413, Iapetus, Ibaiar2306, Infinoind, Inter, Iriseyes, Isaak Dupree, Itai, Itusg15q4user, Ixfd64, J.delanoy, JLaTondre, JPLERouzic, Ja 62, Jamesday, Jamesscho, Jamessungjin.kim, Janzert, Jdthood, Jesse Viviano, Jessel, Jiang, Jnavas, JocelynDelalande, Joerg Reiher, John Smith 104668, John of Reading, Johntheslade, Jonv112, Jonverve, Joshua Scott, Jsaledo, Juanjohn, Justjohnny, KYSoh, Ka-Ping Yee, Kaihsu, Karada, Karenje, Karlshea, Karn, Kbrose, Kc7rad, KelleyCook, Kelly Martin, KevinDorekens, Kgflleischmann, Kgrr, Kharker, Khatru2, Khukri, Kingsley16, Koman90, Kord, Kozuch, Kristen Eriksen, Kunz506, Kurt Jansson, Kvng, Kyle Barbour, LA2, LOL, La goutte de pluie, LachlanA, Lag10, Lakers, Lambiani, Lambyte, Larry V, Lawrence Cohen, Le Sage, Lee Daniel Crocker, Lee J Haywood, Leotohill, Lfwlfw, Liebeskind, Lightmouse, LittleDan, LittleOldMe old, Llort, Lmatt, Loraan, LordJumper, LuisVilla, Lzur, M1 essam, MK8, Mailer diablo, Mange01, Martin Blank, Martopp, Materialscientist, Matt Crypto, MattSH, Mattsday, Mauro Bieg, Mav, Mebden, Mentifisto, Mgolden, Mhannigan, Michal.feix, Mifter, Mike moreton, Mike1024, Mikeblas, Mikemurphy, Mikeygnyc, Mindbuilder,

Mindmatrix, Minkus, Minna Sora no Shita, Mitsuhirato, Mjmarcus, Mjrichardson1, Mkeating24, Mkrist, Mmccalpin, Mmx1, Modster, Mortein, Mr. Zarniwoop, Msadaa, Msauve, Mulad, MureninC, Muukalainen, Mwarren us, NJA, NailPuppy, Nakon, Nasa-verve, Navinveenu, Nbarbettini, NetRoller 3D, Nick, Nickshanks, Nicoli nicolivich, Nido, Nikita Borisov, Nilolab, Ninly, Njh@bandsman.co.uk, Nnemo, Nneonneo, Nothlit, Nuance13x, Nuno Tavares, Octahedron80, OlEnglish, Olivier, Omegatron, Onsl, Opelio, OpenCommunications, Oriondriver, Orrc, Oscabat, OverlordQ, PacoBell, Panarchy, Pandikarthikanmani, Patrick, Paulc206, Pbyeooh, Pegship, Perey, Peruvianllama, Peter S., Peyre, Pgdn002, Phandel, Phantomdj, PhilHibbs, Philip Trueman, Philtheow, Phoebe, Plasticup, Plugwash, Popapuze, Project2501a, Proska, PseudoSudo, PsyberS, Pt, Puffin, QuantumEleven, Quasipalm, Qwertyshan, R6144, RJHall, Rabbeinu, Radioraiders, Radiosband, Rapomon, Rebel, Recognizance, RedWolf, Rednectar.chris, Renegadeviking, RexNL, Rfl, Rhobite, Rich Farmbrough, Richwales, Rick Sidwell, Rjairam, Rjwilmsi, Rlevse, Roadrunner, RobNick, Robert K S, Robert Merkel, Robertoalencar, Ronz, Rossami, Roybadami, Rppr, Rrburke, Rsm9883, Rufous, S, S.smith.1-398, S1N3d dW17, SSTwinrova, Sa.vakilian, SamJohnston, Samuella, Sandeshgoel, Sandos, Sandox, Sargent, Sarpkaya92, Sathaksela, Sceptre, Schapel, ScIm, Scohoust, Seaneose, Sfoskett, Shadowjams, Shanafme, Shanel, Shaper252, Shibboleth, Shoveldude, Sietse Snel, Signalhead, Sintaku, Sir Lothar, Skor, Skybor, Skyrcall, Slearl, Slitete, Slowking, Man, Slobertson, Soap, Solarisphere, Some jerk on the Internet, Soumyasch, Soupmix, Spk, Speciu5, Speleemann, Spitfire, Splash, Spymanut, Srleffler, Srvmdl, Stecoetze, Stefpap, Stephan Leeds, Stephen Bain, Stephen Gilbert, Steve03Mills, Stewardb, StrengthOfNations, Subharanjan, Suruena, Swiverl, Syndicate, Synthetik, Sysin, TRauMa, TakuyaMurata, Tarquin, Tekeyman, Tgritchie, The Anome, The Epop, The Thing That Should Not Be, TheGerm, TheWeakWilled, Thenickduke, Think outside the box, Thisisborin9, Thue, Tide rolls, Timl2k4, Todd Vierling, Too Rag, Tomh009, Tonsofpcs, TonyW, Travelingseth, Treekids, Trenton11gs, Tsunaminoai, Twthmoses, Twyaii, Uncle Milty, Unused0025, Vanished user psdfiwnet3niurunfuh234rubfwdb7, Vaughan Pratt, VdSV9, Vegaswikian, Velella, VerticalAsymtote, Vipintm, Vlad, W Nowicki, WCat, Warren, Waveguy, Wavelength, Waveletrules, Wavyriver, Widefox, Will Beback, Willy on Wheels over Ethernet, Winterspan, Wphilipw, Wrs1864, Wtshymanski, WulfTheSaxon, Ww, Wysprgr2005, X-Destruction, XSG, Xaosflux, Xichael, Xmemonic, Y2kboy23, Yamaguchi先生, Yandman, ZeroOne, Zippy, Zr2d2, Yümrü5e, 1601 anonymous edits

**IEEE 802.11 (legacy mode)** Source: <http://en.wikipedia.org/w/index.php?oldid=504298924> Contributors: 16@r, Austin512, ChrisGaultieri, Cybercobra, Dawnseeker2000, Jhansonxi, KelleyCook, Kinema, Sam8, Samwbl123, 4 anonymous edits

**IEEE 802.11a-1999** Source: <http://en.wikipedia.org/w/index.php?oldid=508559934> Contributors: Bomazi, Crissov, Dawnseeker2000, Dougbateman, Eliemer, Falkomry, Fudoreaper, Haaninjo, Jtact, KelleyCook, Leuko, Lissajous, Mange01, Nasa-verve, Rrror, Stephan Leeds, StrengthOfNations, TheNewPhobia, Thunderbird2, Tombomp, Tonny3k, WiFiEngineer, Y717, 35 anonymous edits

**IEEE 802.11b-1999** Source: <http://en.wikipedia.org/w/index.php?oldid=508560139> Contributors: AS, Brian Kendig, DBigXray, Dawnseeker2000, Dirkbb, Ejay, Fram, Gary King, GregorB, Guoguo12, Guy Harris, Haaninjo, Hbent, JohnCD, KelleyCook, Kf4yfd, Kvng, LiHelpa, Loupeter, Madkayaker, Mindmatrix, Nasa-verve, Octahedron80, Oli Filth, R'n'B, Sandman q23, StrengthOfNations, Tim-mnm, Tskandier, Woohookity, Y717, 40 anonymous edits

**IEEE 802.11g-2003** Source: <http://en.wikipedia.org/w/index.php?oldid=508560095> Contributors: Airplaneman, Alethiophile, Angielaj, Blissreader, Cecilyen, Dawnseeker2000, Haaninjo, Jesse Viviano, Kauczuk, KelleyCook, Kf4yfd, Mange01, Mindmatrix, Nasa-verve, Networkingguy, NoCal100, Rchandra, Ryoga Godai, Sandman q23, Staeiou, Steve2011, StrengthOfNations, Tellthepeople, Thunderbird2, Tim-mnm, Tskandier, Y717, 44 anonymous edits

**IEEE 802.11n-2009** Source: <http://en.wikipedia.org/w/index.php?oldid=509084299> Contributors: Static, 802dot11n, 802geek, Addykins, Alansohn, Alfaisanomega, Anaxial, Antonio Lopez, Arakunem, Arichnad, Armyable, AssetBurned, Aussiejohn, AzaToth, Bastian.Bittorf, Brianski, Bubba73, Buxtehude, Camw, Cassowary, CecilWard, CerysH, Chowbok, Chrisch, CitizenDAK, Clerks, CyberSpark, Cybercobra, Dancter, Danhash, Daniel.Cardenas, Dannycrouch, Danroa, DeadEyeArrow, Deli nk, DenisYurkin, Dijg2006, Dmarrquard, Dogcow, Download, DragonHawk, Dwarfpower, EAi, Ejay, Elessar, Euku, FashionNugget, Flurry, Foreverstroked, Fudoreaper, Gail, Gmoose1, Goto, Guy Harris, HITChair, Haaninjo, HenryLarsen, Hitechgrl, Husoku, IWCaldwell, Int21h, Ioda006, Itusg154user, JBsupreme, JHP, Jalal0, JamesPaulWhite, JasonAQuest, Jimthimg, Joejava, Jonjames1986, Joshua Issac, Jsc, Juicecowboy, KelleyCook, Kgrr, Kozuch, Kvng, LMB, LOL, Lightmouse, LiHelpa, Little Professor, Lousyd, Mange01, Mazin07, MichaelStanford, Monkeyblue, Monster12, Nasa-verve, NetRoller 3D, Nux, Onesimos, Oosh, OpenCommunications, PacoBell, Paulgur, PeterEassthope, Phandel, Pmantilla, Pol098, Radical Mallard, Remember the dot, Rjwilmsi, Romark, SGMD1, Sandeshgoel, Sandman q23, Scott English, Scottmacpherson, Scottman1995, Scott9, Sdorman, Sdwood, Sellwireless, ShakataGaNai, Silvers, Sligocki, Sloopjk, SnowDrgn, Stephan Leeds, Stephantom, Steve03Mills, StrengthOfNations, Subversive.sound, Thbotch, Themusicod1, Thurperward, Tjking45, Umonofia, V35b, Voidxor, Wasint, Wavyriver, Wg206, WiFiEngineer, WikHead, Winvista64, Woottoo, Wtmitchell, XP1, Xaj0, Y717, Yellowdesk, Zappix, Zehawk, 237 anonymous edits

**Twisted pair** Source: <http://en.wikipedia.org/w/index.php?oldid=509350488> Contributors: Adam78, Adamantios, Aeons, Ahamedshake, Alan Parmenter, Aldie, Alemily, Algoco, Amillar, AnkhMorpork, Annabcn8, Anon lynx, Anon user, ArnoldReinhold, Azucchinali, Bachrach44, Biblbroks, Binksternet, Bje2089, Bobo192, Borgx, BrokenSegue, Brownings, Brucevdk, Btlm, Bungalowbill, BweeksLSLU, CEdmundo, Cabling guy, Calamarain, CalumH93, Casey Abell, Cburnett, Chldzy, Chill doubt, Cjdkok, Clemwang, CosineKitty, Courcelles, Cyril.holweck, Dabeau, DanO256, Danutz, DarkShroom, Dbest123456, Dc3, Deelkar, Deepakindori, Diflock, Dispenser, DjfbFire, Don Cuan, Dougofborg, Dpotter, Ebayabe, Elaragirl, Eleanor1975, Enviromet, Excirial, Fieldday-sunday, Fooobar, FormulaX, Fred J, Gah4, Garycompugeek, Giftlite, Giomonic, GreenSpigot, Greensburger, Greudin, Habahn hanuka, Hamish28, Happenstancial, Harryboyles, Harryzilber, Hatechurch, Head, Hede2000, Heron, Hosterweis, Hrvatistan, I dream of horses, Ida Shaw, Intr, Itpastorn, J.delanoy, Jackol, Jdigangi, JensRex, Jftaylor21, Jim.henderson, Jim1138, Jjeka, Johnuniq, JonHarder, Jovianeye, Julesd, Juliancolton, Juliano, KelleyCook, Klaus100, Koman90, Kvng, Lee Carre, Lilianag, Lmatt, LoopTel, Lou.weird, Lradrama, Lunaverse, MER-C, Magnus.de, Manuel Anastacio, Maureen, Mboverload, Michael Frind, Mmmeg, Mortense, Moverton, Mozzera, Mrand, Myanw, NTox, Nachomann-a, NawlinWiki, Neil916, NewEnglandYankee, Nhamor, Nifky?, Novatek, Omegatron, Opelio, Phantomsteve, Piano non troppo, Pmsyyz, Poweroid, Psinu, Pumba80, Qirex, R'n'B, Radiojon, Ranveig, Rfl, Rich Farmbrough, Rossumcapek, Rrburke, SDC, Savant13, Seaphoto, Shaddack, Chanel, Shayan025, Sho Uemura, Skiguy145, SlipperyHippo, Snafflekid, Snori, Spinningspark, Srleffler, Steelpillow, Stephan Leeds, Stephenb, Svgabertian, Tad Lincoln, The Anome, The Thing That Should Not Be, TheAMmollusc, Thewebdruid, Thexchair, Thinggg, Tide rolls, TimmyGUNZ, TinyMark, Tom harrison, TommyG, Toresbe, Tothwolf, VT hawkeye, Vy0123, Wasacz93, Wendt, Wernher, Witlinckx, Williamv1138, Willy on Wheels over Ethernet, Wimt, Wolfkeeper, Wowbagger42, Woz2, Wtshymanski, XL2D, Yurik, ZeroOne, Zidonuke, Zoicon5, Zojj, 432 anonymous edits

**Optical fiber** Source: <http://en.wikipedia.org/w/index.php?oldid=509558892> Contributors: 123davidn, 130.161.103.xxx, 28421u2232nfencenc, 2D, 4twenty42o, 63.192.137.xxx, 7, 8472, A little insignificant, A. B., A. d. M., A3RO, A876, AThing, Aaron Brenneman, Aaron.peache3, Abgodfrey, Abhishek191288, Abhishekroy, 2jan, AbstractEpiphany, Acalamari, Ackbeet, Adam Schwing, Adamantios, Adambro, Afluegel, Ahoersteemeier, Atilias, Alansohn, Alasdair, Alasdairhurst, Alby, Aldie, Al jrh, Alandro, Altemann, Alvestrand, Alyssa.needham, Alyssaprv, Amps, Andonic, AndrewP7891, Andrewrp, Andycipj, Anetode, Anon lynx, Anonymousaaa, Antonio.napoli, Anyadelarose, Arastep, Art LaPella, Arx Fortis, Atif.t2, Atlant, Atrius, AubreyEllenShomo, Avono, AwamerT, AxelBoldt, Axelman99, Axiosaurus, Aymath2, Azteciv, B Milnes, Backpackadam, Baggio10, Bakilas, Baloo rch, Barosaurus Lentus, Baskoropratomo, Basvbl, Batsell, BenFrantzDale, Bender235, Beneluxus, Bensmooth10, Bert490, Billaje123, Birge, Biscuitin, BlaKE, Blaxthos, Blue bear sd, Bob House 884, Bobblewik, Bobo192, Bonazi, Bongwarrior, Bookofjude, BorgQueen, Boundary11, Brabo, Brianga, Bruce Elphinston, Robertson, Bryan Derkser, Bubbleboys, Burntsauce, Cable master, Cactus, Cattus, Caiaffa, Callan Oakeshott, CanadianLinuxUser, Capricorn42, Capt. James T. Kirk, Captain-n00dle, CaptainRon, CaptainVindaloo, CfIm001, Cgbraschi, Chairman S., Chamal N, Chaosfeary, Cheakamus, Chenggong, Chetvorno, Chris Howard, Chris Roy, Chris the speller, Chris55, Christko, Christofferdupont, Christopher Parham, Chriswiki, Ctteam, Clappingsimon, Cmdrjameson, Cokoli, Colin Marquardt, ColinEberhardt, Colonies Chris, Colorador, Comisat, Connectel, Conversion script, Corinne68, CorpX, Correogsk, Courcelles, Cowicide, Crazycomputers, Crvenotopce, Csi295, Ctry36, Cuhlik, DARTH SIDIOUS 2, DKwerty, DMB, Dmacks, DVD R W, Daderot, Dagus2000, DancingPenguin, Dandin1, Daniel C, Daniel Callejas Sevilla, Daniel Olsen, DanielICD, Danny123434, Darrel francis, Darth Panda, Davidgothberg, Davidprior, Dbkeck, Dbunker, Dee194, Deljr, Dcoolt, De728631, DeadEyeArrow, Deborahhockham, Deeptrivia, Degrl6328, Deiz, Dekisugi, Deor, DerHexer, Dgw, Dicklyon, Dima373, Dinapurnasari, Dirgela, Djames, Djan4961, Dlohcirekin, Doesnae, DonPMitchell, Dor, Dougofborg, Dr John Wells, DrBob, Dreadstar, Dscharrer, Dthomson8, Duffy2006, Dwains1959, Dyspres, EIFY, EagleFan, Edcolins, Edgardo, Editor at Large, EdoDodo, Elaragirl, ElectricEye, Elockid, EncourageThe Wind, Entropy, Epbr123, Erianna, Eric Kvaelan, Estel, Etan J, Tal, Euryalus, Everything, Evilhunter, Ewlyahoocon, Exacerbation, Excirial, Exsequor, Eyeoteye, FF2010, FastLizard4, Fdilodilo, Felyza, Femto, Fiber-optics, Fieldday-sunday, FinalRapture, Finchsnows, Fitzcollings, Footwarrior, Fountains of Bryn Mawr, Foxj, Francis Flinch, Fulldcent, Funandrvl, Fuzheado, Gamer007, Ganesh Paudel, Gascreed, Gayhunter, Gene Nygaard, Genesiscode, Gerry Ashton, Gfoley4, Giftlite, Gioto, GirasoleDE, Glenn, Gogo Dodo, Graeme Bartlett, Graemel, GrafZahl, Graham87, Grahame, GreatMizti, GregorB, Gringer, Gritzko, Hadal, Hamid002.2008, Harikatukutu, Harryzilber, Hasanalun, Hayabusu future, Hcsrn, Hdoren, Hendersonjace, Hephaestos, Hereforhomework2, Hermant patel, Heron, HexaChord, Highvoltage123, Hm369, Hojar, Hon-3s-T, Hooria, Hu12, Hustvedt, I already forgot, IceKarma, Igiffin, Igoldeste, Imellor, Imperfection, Inbamkumar86, Iner22, Infinity Spiral, Inoen, Intr, Inthenet, Invincible Ninja, Iohannes Animosity, Iridescent, Itai, Ivan Akira, Ixymapeo, J.P.Lon, J.delanoy, JForget, JNW, JTAN, JZDA, Jackfork, Jamsignal, Jason One, Javierito92, Jcc2011, Jeevesness, JefeMixtli, Jeff G., Jenjong9, Jflabourdette, Jim.henderson, Jim1138, Jock Boy, Joe9320, Joefaust, John, JohnGray, JohnTechnologist, Johnpseudo, Jono489654e5e, Jordgette, Jovianeye, Jpfägerback, Jpgordon, Jrvz, Jsnow, Jstahley, Juliancolton, Jusdrafax, KDesk, Ka Faran Gatri, Karada, Kathryn NicDhána, Kc307, Keithdsilva, KelleyCook, Kevinkph85, Kingpin13, Klaus100, Krellis, Kristen Eriksen, Kukini, Kunallanjewar, Kungfuadam, Kvng, Kwiki, L Kensington, LA2, LFW, LG4761, Laboriusdude, LachlanA, Lahiru k, LalahGrace, Lambda dog, Landroo, Lars Washington, LeaveSleaves, Lee Carré, Lee317, Leon7, Leszek Jańczuk, Liao, LightSword, Lighthouse, LiiHelp, Lilianag, Linnell, Linuxrules1337, Lizgo, LjkCa, Lmatt, Logger9, Loren36, LostSole, Lotu, Lowellian, Luk, Luna Santin, MER-C, Machine123, Mackwho, Macy, Magnus.de, Maksud, Manco Capac, Mani1, Manigo, Marc Lacoste, Marek69, Maria Poise, Marshall Williams2, Martijn Hoeckstra, MartinHarper, Mascotmayank, Matdrodes, Materialscientist, Matnkat, Matthew kokai, Matisse, Maximus Rex, Mblumber, Mbvanleeuwen, McGeddon, Melena, Mencel, Metacomet, Mfv2, Mgiganteus1, Mhare, Michael Hardy, Michaelflorida@yahoo.com, Michilans, Mindmatrix, Minimac, Miniscus77, Mion, Mirror Vax, MisterSheil, Moreschi, Mpisray, Mr. Lefty, Mrba70, Mrmnty, Mtmcbs, MureninC, Mushroom Man, Music Sorter, Mwanmer, Myanw, NUNAL SA MUKHA NI GLORIA, Narayan82es, Nasa-verve, Navigatr85, NawlinWiki, Neckermane, Neilc, NellieBly, NeoChaosX, Nick, Nick Number, Nick2588, Nikevich, Nikvist, Nimbusania, NittyG, Nk, Northsun, Nutiketaiel, Oberst, Oblivious, Ojay123, Old Moonraker, Oliver202, OllieFury, Opticana, Optics2006, Outrigr, Pabix, Palthainon, Pam.howie, Panarchy, Patrick Berry, Pavel Voznenilek, Peizo, Peterlewis, Petiatil, Petr, Pfoarde, Phadippides, Phantomsteve, PhilKnight, Philip Truman, Philippe, Phillipedison1891, Photoniqe, Pick45, Pinkbasu, PiperArrwon3191q, Pippin Bear, Pjpvip, Polymorph, Porqin, Prokopenya Viktor, Psitusa, Putri Rizki, QuantumEleven, R'n'B, RPGMarker35, RPschottar, Rahul s ind, RasefC, Rawlder, Ray Van De Walker, ReallyNiceGuy, Reaper X, Reconsider the static, RedTony, RedWolf, Redeem, ResearchRave, RexNL, Reywas92, RichAromas, Richard Arthur Norton (1958- ), Richard.decal, Richmd, Rick Sidwell, Rightcolour, Rjd0060, Rjwilmsi, Rmosler2100, Robchurch, Ronebofh, Royboycrashfan, Rrburke, Rriissa, Rvolz, Ryanrs, S Roper, Sbijou, Saiarcot895, Salsa Shark,

Sbarnard, SchfiftyThree, SchnozToiger, SchreyP, Schohurst, ScottyBerg, Seanwal111111, Searchme, Secarrie, Senor Cuete, Seraphim, Sergiusz Patela, Serych, Shaddack, Shadow demon, Sharifaly, Shniken, Shoeofdeath, SilkTork, Silly rabbit, SimonP, Simplejacktard, Siphlab, Skateer2, Skkies, SlimVirgin, SloppyNick, Smallman12q, SoCalSuperEagle, Socceroos, Some standardized rigour, SpK, Spitfire, Srleffler, Stephenchou0722, Stickred, Storm Rider, Strait, Stratocracy, Studious91, Studust, Sun Creator, Sundae, SuperHamster, Surpluseq, Surv1v4l1st, Swpb, TDogg310, THEN WHO WAS PHONE?, Tabletop, Talkstosocks, Tanner0259, Tarchon, Tarret, Td93, TechnoOptics, Ted BJ, Teketime, Texnic, That Guy, From That Show!, The Anome, The Epop, The Firewall, The Photon, The Thing That Should Not Be, The man stephen, TheAMmollusc, TheFOA, TheOldJacobite, Thewalrus, Things, Thiseye, Thumperward, Thunderbird2, Thunderboltz, Thunderstrike353582, Tiddly Tom, Tide rolls, Tim Starling, Timbercon, Timwether, Timwi, Titopao, Tmarquee, Tobias Ahl, Tomchiuke, Tomcritchlow, Tommy2010, Toussaint, Traxs7, Triplelutz, Trumpetcat6, Trusilver, Tsunenet, Twang, Uhai, Unregistered.coward, User A1, Utcurusch, Ut in DC, UtherSRG, V.narsikar, Valterforesto, Vectorsoliton, Velella, Verbalcontract, Versus22, VictorAnyakin, Vilding1, Vonspringer, Vrenator, Vssun, W.Hylla, WCroslan, Wafulz, Wasell, Wavelength, Waxigloo, Wayward, Webwat, Wereon, West.andrew.g, Weviwevi, Wik1ped1a is meant 2 be vandalised, WikiWikiPhil, Wikieditor06, Wikipelli, Willidarski, Wint, Wj32, WIfootball, Wolfkeeper, Woohookitty, Wozniak1337, Wyf2012, X!, X42bn6, XLerate, Xaosflux, Xnuala, Yamamoto Ichiro, Yekrats, Yerpo, Yoasaine, Ytrottier, Zhitya, Zondor, Zvn, Zwz8406, تاریخ نویری, 1589 anonymous edits

**Optical fiber connector** *Source:* <http://en.wikipedia.org/w/index.php?oldid=509545348> *Contributors:* 123davidn, 12Gooner89, A. B., Adam850, Adamantios, Akadruid, Alecv, Aleks-eng, Amirrad.en, Andy M. Wang, Anna Lincoln, Ayla, Bamyers99, Basketeur12, BenFrantzDale, Bert490, Blaragh2015, Bobo192, Bruce Elphinston Robertson, Buthunter, Buthunters, Canterbury Tail, Chaosfeary, CommonsDelinker, Ctbolt, Darth Panda, Datsyuk, DrBob, DragonHawk, Dustin gayler, DynamoDegsy, Fb35523, GWS EE, Grahame, Gurnec, Heywoð, JNW, Jamieginsberg, Jim.henderson, Jkellow, Joy, Katkins84, Kirnehkrib, Maqian163, McHildinger, Michael Hardy, Michilans, Mikm, Mild Bill Hiccup, Mindmatrix, MitchellShnier, Nicolaasuni, PL290, Pfagerburg, Philip Trueman, Pmaunz, Quadell, R'n'B, Rajee vran, Res2216firestar, Rkarlsba, Rohieb, Ronz, S Roper, Sallyfiber, Shadowjams, Simonebaldassari, Skeetabomb, Sophus Bie, Sparkle Ulawe, Srice13, Srleffler, Stephan Leeds, Svaliga, Telcoterry, The wub, TheFOA, Timbercon, WCroslan, Wayne Slam, Wtshymanski, Wyf2012, Ytrottier, Zhuliangzhuiang, 145 anonymous edits

# Image Sources, Licenses and Contributors

**File:Distributed Processing.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Distributed\\_Processing.jpg](http://en.wikipedia.org/w/index.php?title=File:Distributed_Processing.jpg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Bp2010.hprastiawan

**File:Internet map 1024.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Internet\\_map\\_1024.jpg](http://en.wikipedia.org/w/index.php?title=File:Internet_map_1024.jpg) *License:* Creative Commons Attribution 2.5 *Contributors:* Barrett Lyon The Opte Project

**File:NETWORK-Library-LAN.png** *Source:* <http://en.wikipedia.org/w/index.php?title=File:NETWORK-Library-LAN.png> *License:* Creative Commons Attribution 3.0 *Contributors:* Heberkowitz

**File:EPN Frame-Relay and Dial-up Network.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:EPN\\_Frame-Relay\\_and\\_Dial-up\\_Network.svg](http://en.wikipedia.org/w/index.php?title=File:EPN_Frame-Relay_and_Dial-up_Network.svg) *License:* Creative Commons Attribution-Share Alike *Contributors:* Ludovic.ferre

**File:Virtual Private Network overview.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Virtual\\_Private\\_Network\\_overview.svg](http://en.wikipedia.org/w/index.php?title=File:Virtual_Private_Network_overview.svg) *License:* Creative Commons Attribution-Share Alike *Contributors:* Ludovic.ferre

**File:Network Overlay.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Network\\_Overlay.svg](http://en.wikipedia.org/w/index.php?title=File:Network_Overlay.svg) *License:* Creative Commons Attribution-Share Alike *Contributors:* Ludovic.ferre]]

**Image:PD-icon.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:PD-icon.svg> *License:* Public Domain *Contributors:* Alex.muller, Anomie, Anonymous Dissident, CBM, MBisanz, PBS, Quadell, Rocket000, Strangerer, Timotheus Canens, 1 anonymous edits

**Image:Ethernet.png** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Ethernet.png> *License:* GNU Free Documentation License *Contributors:* Ilario, Ustas

**File:LAN WAN scheme.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:LAN\\_WAN\\_scheme.svg](http://en.wikipedia.org/w/index.php?title=File:LAN_WAN_scheme.svg) *License:* Creative Commons Attribution-ShareAlike 3.0 Unported *Contributors:* Gateway\_firewall.svg: Harald Mühlböck derivative work: Ggia (talk)

**Image:WI-FI Range Diagram.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:WI-FI\\_Range\\_Diagram.svg](http://en.wikipedia.org/w/index.php?title=File:WI-FI_Range_Diagram.svg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* WI-FI\_Range\_Diagram.png: robo56 (talk) Original uploader was Robo56 at en.wikipedia derivative work: B. Jankuloski (talk)

**File:CDSC wifi Classon jeh.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:CDSC\\_wifi\\_Classon\\_jeh.jpg](http://en.wikipedia.org/w/index.php?title=File:CDSC_wifi_Classon_jeh.jpg) *License:* Creative Commons Zero *Contributors:* Jim.henderson

**Image:HotSpot pay phone at Hafenbahnhof Friedrichshafen.JPG** *Source:* [http://en.wikipedia.org/w/index.php?title=File:HotSpot\\_pay\\_phone\\_at\\_Hafenbahnhof\\_Friedrichshafen.JPG](http://en.wikipedia.org/w/index.php?title=File:HotSpot_pay_phone_at_Hafenbahnhof_Friedrichshafen.JPG) *License:* Creative Commons Attribution-Sharealike 3.0,2.5,2.0,1.0 *Contributors:* Davidmoerike

**Image:User Fairness Model02.png** *Source:* [http://en.wikipedia.org/w/index.php?title=File:User\\_Fairness\\_Model02.png](http://en.wikipedia.org/w/index.php?title=File:User_Fairness_Model02.png) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Hermann Pommer

**Image:User Fairness Model01.png** *Source:* [http://en.wikipedia.org/w/index.php?title=File:User\\_Fairness\\_Model01.png](http://en.wikipedia.org/w/index.php?title=File:User_Fairness_Model01.png) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Hermann Pommer

**File:OSI-model-Communication.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:OSI-model-Communication.svg> *License:* Public Domain *Contributors:* RuntuX

**Image:Spanning tree protocol at work 1.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Spanning\\_tree\\_protocol\\_at\\_work\\_1.svg](http://en.wikipedia.org/w/index.php?title=File:Spanning_tree_protocol_at_work_1.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* GhosT

**Image:Spanning tree protocol at work 2.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Spanning\\_tree\\_protocol\\_at\\_work\\_2.svg](http://en.wikipedia.org/w/index.php?title=File:Spanning_tree_protocol_at_work_2.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* GhosT

**Image:Spanning tree protocol at work 3.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Spanning\\_tree\\_protocol\\_at\\_work\\_3.svg](http://en.wikipedia.org/w/index.php?title=File:Spanning_tree_protocol_at_work_3.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* GhosT

**Image:Spanning tree protocol at work 4.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Spanning\\_tree\\_protocol\\_at\\_work\\_4.svg](http://en.wikipedia.org/w/index.php?title=File:Spanning_tree_protocol_at_work_4.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* GhosT

**Image:Spanning tree protocol at work 5.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Spanning\\_tree\\_protocol\\_at\\_work\\_5.svg](http://en.wikipedia.org/w/index.php?title=File:Spanning_tree_protocol_at_work_5.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* GhosT

**Image:Spanning tree protocol at work 6.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Spanning\\_tree\\_protocol\\_at\\_work\\_6.svg](http://en.wikipedia.org/w/index.php?title=File:Spanning_tree_protocol_at_work_6.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* GhosT

**Image:TCP/IP 802.1Q.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:TCP/IP\\_802.1Q.jpg](http://en.wikipedia.org/w/index.php?title=File:TCP/IP_802.1Q.jpg) *License:* Public Domain *Contributors:* Arkrishna

**Image:TCP/IP 802.1ad DoubleTag.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:TCP/IP\\_802.1ad\\_DoubleTag.jpg](http://en.wikipedia.org/w/index.php?title=File:TCP/IP_802.1ad_DoubleTag.jpg) *License:* Public Domain *Contributors:* Arkrishna

**Image:802.1X wired protocols.png** *Source:* [http://en.wikipedia.org/w/index.php?title=File:802.1X\\_wired\\_protocols.png](http://en.wikipedia.org/w/index.php?title=File:802.1X_wired_protocols.png) *License:* GNU Free Documentation License *Contributors:* Arran Cudbard-Bell Arr2036

**Image:Ethernet RJ45 connector p1160054.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Ethernet\\_RJ45\\_connector\\_p1160054.jpg](http://en.wikipedia.org/w/index.php?title=File:Ethernet_RJ45_connector_p1160054.jpg) *License:* Creative Commons Attribution-ShareAlike 3.0 Unported *Contributors:* User:David.Monniaux

**File:Loudspeaker.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Loudspeaker.svg> *License:* Public Domain *Contributors:* Bayo, Gmaxwell, Husky, Iamunknow, Mirithing, Myself488, Nethac DIU, Omegatron, Rocket000, The Evil IP address, Wouterhagens, 20 anonymous edits

**File:10Base5transcivers.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:10Base5transcivers.jpg> *License:* Creative Commons Attribution-Sharealike 2.5 *Contributors:* Original uploader was Robert.Harker at en.wikipedia

**Image:Network card.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Network\\_card.jpg](http://en.wikipedia.org/w/index.php?title=File:Network_card.jpg) *License:* GNU Free Documentation License *Contributors:* User:Nixdorf

**File:Network switches.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Network\\_switches.jpg](http://en.wikipedia.org/w/index.php?title=File:Network_switches.jpg) *License:* unknown *Contributors:* ShakataGaNaI

**File:Coreswitch (2634205113).jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Coreswitch\\_\(2634205113\).jpg](http://en.wikipedia.org/w/index.php?title=File:Coreswitch_(2634205113).jpg) *License:* Creative Commons Attribution-Sharealike 2.0 *Contributors:* Dave Fischer

**File:Link Aggregation1.JPG** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Link\\_Aggregation1.JPG](http://en.wikipedia.org/w/index.php?title=File:Link_Aggregation1.JPG) *License:* Public Domain *Contributors:* HammondJr

**File:PoE Access Point v2.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:PoE\\_Access\\_Point\\_v2.jpg](http://en.wikipedia.org/w/index.php?title=File:PoE_Access_Point_v2.jpg) *License:* Public Domain *Contributors:* myself

**Image:1140E.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:1140E.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Geek2003

**File:5520-24-POE.JPG** *Source:* <http://en.wikipedia.org/w/index.php?title=File:5520-24-POE.JPG> *License:* GNU Free Documentation License *Contributors:* Darth Panda, PassportDude, Shell Kinney, 3 anonymous edits

**File:Intel PRO-1000 GT PCI NIC.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Intel\\_PRO-1000\\_GT\\_PCI\\_NIC.jpg](http://en.wikipedia.org/w/index.php?title=File:Intel_PRO-1000_GT_PCI_NIC.jpg) *License:* Public domain *Contributors:* ktims (talk). Original uploader was Ktims at en.wikipedia

**Image:Intelpromtserverpcixadapter1000mta342.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Intelpromtserverpcixadapter1000mta342.jpg> *License:* Public Domain *Contributors:* Original uploader was Spc01 at en.wikipedia

**File:Avaya-10G-ERS-8600.png** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Avaya-10G-ERS-8600.png> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Geek2003

**Image:Intel XFP.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Intel\\_XFP.jpg](http://en.wikipedia.org/w/index.php?title=File:Intel_XFP.jpg) *License:* Public Domain *Contributors:* CerberuS

**File:Netiron xmr 16000.JPG** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Netiron\\_xmr\\_16000.JPG](http://en.wikipedia.org/w/index.php?title=File:Netiron_xmr_16000.JPG) *License:* Creative Commons Attribution 2.5 *Contributors:* おむこさん志望

**Image:Ipv4 address.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Ipv4\\_address.svg](http://en.wikipedia.org/w/index.php?title=File:Ipv4_address.svg) *License:* Public Domain *Contributors:* Indeterminate

**Image:Ipv6 address.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Ipv6\\_address.svg](http://en.wikipedia.org/w/index.php?title=File:Ipv6_address.svg) *License:* Public Domain *Contributors:* Indeterminate

**File:Tcp state diagram fixed.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Tcp\\_state\\_diagram\\_fixed.svg](http://en.wikipedia.org/w/index.php?title=File:Tcp_state_diagram_fixed.svg) *License:* GNU Free Documentation License *Contributors:* Tcp\_state\_diagram\_new.svg: \*derivative work: Sergiode2 (talk) Tcp\_state\_diagram.svg: dnet derivative work: Marty Pauley (talk)

**File:TCP CLOSE.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:TCP\\_CLOSE.svg](http://en.wikipedia.org/w/index.php?title=File:TCP_CLOSE.svg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Iustitia

**Image:Tcp.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Tcp.svg> *License:* Creative Commons Attribution-ShareAlike 3.0 Unported *Contributors:* Mike de

**File:UDP encapsulation.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:UDP\\_encapsulation.svg](http://en.wikipedia.org/w/index.php?title=File:UDP_encapsulation.svg) *License:* GNU Free Documentation License *Contributors:* en:User:Cburnett original work, colorization by en:User:Kbrose

**File:Ipv4-exhaust.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Ipv4-exhaust.svg> *License:* Creative Commons Attribution-Share Alike *Contributors:* Mro

**File:Rir-rate.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Rir-rate.svg> *License:* Creative Commons Attribution-Sharealike 3.0,2.5,2,0,1,0 *Contributors:* Mro

**File:Huston\_rir\_ipv4\_exhaustion\_projection.png** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Huston\\_rir\\_ipv4\\_exhaustion\\_projection.png](http://en.wikipedia.org/w/index.php?title=File:Huston_rir_ipv4_exhaustion_projection.png) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Thus

**File:Regional Internet Registries world map.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Regional\\_Internet\\_Registries\\_world\\_map.svg](http://en.wikipedia.org/w/index.php?title=File:Regional_Internet_Registries_world_map.svg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Rir,gif: BlankMap-World6,\_compact.svg: Canuckguy et al. derivative work: Sémhur (talk)

**File:Ipv6 address leading zeros.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Ipv6\\_address\\_leading\\_zeros.svg](http://en.wikipedia.org/w/index.php?title=File:Ipv6_address_leading_zeros.svg) *License:* Public Domain *Contributors:* Ipv6\_address.svg: Indeterminate derivative work: BobbyPeru (talk)

**File:World IPv6 launch logo.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:World\\_IPv6\\_launch\\_logo.svg](http://en.wikipedia.org/w/index.php?title=File:World_IPv6_launch_logo.svg) *License:* Creative Commons Attribution 3.0 *Contributors:* Matma Rex

**File:Ipv6 header.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Ipv6\\_header.svg](http://en.wikipedia.org/w/index.php?title=File:Ipv6_header.svg) *License:* Creative Commons Attribution-Sharealike 3.0,2.5,2,0,1,0 *Contributors:* Mro

**File:DHCP Server.png** *Source:* [http://en.wikipedia.org/w/index.php?title=File:DHCP\\_Server.png](http://en.wikipedia.org/w/index.php?title=File:DHCP_Server.png) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Patpat

**Image:Full Cone NAT.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Full\\_Cone\\_NAT.svg](http://en.wikipedia.org/w/index.php?title=File:Full_Cone_NAT.svg) *License:* Creative Commons Attribution-ShareAlike 3.0 Unported *Contributors:* Christoph Sommer

**Image:Restricted Cone NAT.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Restricted\\_Cone\\_NAT.svg](http://en.wikipedia.org/w/index.php?title=File:Restricted_Cone_NAT.svg) *License:* Creative Commons Attribution-ShareAlike 3.0 Unported *Contributors:* Christoph Sommer

**Image:Port Restricted Cone NAT.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Port\\_Restricted\\_Cone\\_NAT.svg](http://en.wikipedia.org/w/index.php?title=File:Port_Restricted_Cone_NAT.svg) *License:* Creative Commons Attribution-ShareAlike 3.0 Unported *Contributors:* Christoph Sommer

**Image:Symmetric NAT.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Symmetric\\_NAT.svg](http://en.wikipedia.org/w/index.php?title=File:Symmetric_NAT.svg) *License:* Creative Commons Attribution-ShareAlike 3.0 Unported *Contributors:* Christoph Sommer

**File:Snmpp.PNG** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Snmpp.PNG> *License:* GNU Free Documentation License *Contributors:* Rene Bretz

**File:SRI First Internetworked Connection diagram.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:SRI\\_First\\_Internetworked\\_Connection\\_diagram.jpg](http://en.wikipedia.org/w/index.php?title=File:SRI_First_Internetworked_Connection_diagram.jpg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Russavia

**File:SRI Packet Radio Van.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:SRI\\_Packet\\_Radio\\_Van.jpg](http://en.wikipedia.org/w/index.php?title=File:SRI_Packet_Radio_Van.jpg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Russavia

**Image:IP stack connections.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:IP\\_stack\\_connections.svg](http://en.wikipedia.org/w/index.php?title=File:IP_stack_connections.svg) *License:* GNU Free Documentation License *Contributors:* en:User:Kbrose

**Image:UDP encapsulation.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:UDP\\_encapsulation.svg](http://en.wikipedia.org/w/index.php?title=File:UDP_encapsulation.svg) *License:* GNU Free Documentation License *Contributors:* en:User:Cburnett original work, colorization by en:User:Kbrose

**Image:IGMP\_basic\_architecture.png** *Source:* [http://en.wikipedia.org/w/index.php?title=File:IGMP\\_basic\\_architecture.png](http://en.wikipedia.org/w/index.php?title=File:IGMP_basic_architecture.png) *License:* Public domain *Contributors:* Harpreet Eighty-Two (Harpreet82 at en.wikipedia)

**Image:SMTP-transfer-model.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:SMTP-transfer-model.svg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Ale2006-from-en

**image:cast.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Cast.svg> *License:* Public Domain *Contributors:* Easys12c

**image:anycast.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Anycast.svg> *License:* Public Domain *Contributors:* Easys12c, H Padleckas, Jarekt, 1 anonymous edits

**image:broadcast.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Broadcast.svg> *License:* Public Domain *Contributors:* Easys12c

**image:multicast.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Multicast.svg> *License:* Public Domain *Contributors:* Easys12c, Lupo, 1 anonymous edits

**image:unicast.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Unicast.svg> *License:* Public Domain *Contributors:* Easys12c, Perhelion

**image:geocast.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Geocast.svg> *License:* Creative Commons Zero *Contributors:* Revolus

**Image:WRT54G\_v2 Linksys Router Digon3.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:WRT54G\\_v2\\_Linksy Router\\_Digon3.jpg](http://en.wikipedia.org/w/index.php?title=File:WRT54G_v2_Linksy Router_Digon3.jpg) *License:* unknown *Contributors:* "Jonathan Zander (Digon3)"

**Image:2.4 GHz Wi-Fi channels (802.11bg WLAN).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:2.4\\_GHz\\_Wi-Fi\\_channels\\_\(802.11bg\\_WLAN\).svg](http://en.wikipedia.org/w/index.php?title=File:2.4_GHz_Wi-Fi_channels_(802.11bg_WLAN).svg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Michael Gauthier, Wireless Networking in the Developing World

**Image:NonOverlappingChannels2.4GHzWLAN-en.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:NonOverlappingChannels2.4GHzWLAN-en.svg> *License:* Creative Commons Attribution 3.0 *Contributors:* Liebeskind

**File:2.4 GHz Wi-Fi channels (802.11g WLAN).svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:2.4\\_GHz\\_Wi-Fi\\_channels\\_\(802.11g\\_WLAN\).svg](http://en.wikipedia.org/w/index.php?title=File:2.4_GHz_Wi-Fi_channels_(802.11g_WLAN).svg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* 2.4\_GHz\_Wi-Fi\_channels\_(802.11g\_WLAN).svg: Michael Gauthier, Wireless Networking in the Developing World derivative work: MarkWarren (talk)

**Image:25 pair color code chart.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:25\\_pair\\_color\\_code\\_chart.svg](http://en.wikipedia.org/w/index.php?title=File:25_pair_color_code_chart.svg) *License:* GNU General Public License *Contributors:* Pumbaa80, Rocket000, Tothwolf, WikipediaMaster

**Image:WireTransposition.png** *Source:* <http://en.wikipedia.org/w/index.php?title=File:WireTransposition.png> *License:* Creative Commons Attribution-Sharealike 2.5 *Contributors:* Original uploader was LoopTel at en.wikipedia

**File:UTP-cable.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:UTP-cable.svg> *License:* GNU Free Documentation License *Contributors:* Original: Uwe Schwöbel (de:Datei:UTP-Kabel.png) English translation: Deelkar (File:UTP-cable.png) Vector conversion: Sgalbertian

**Image:UTP cable.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:UTP\\_cable.jpg](http://en.wikipedia.org/w/index.php?title=File:UTP_cable.jpg) *License:* Public Domain *Contributors:* Baran Ivo

**Image:FTP cable3.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:FTP\\_cable3.jpg](http://en.wikipedia.org/w/index.php?title=File:FTP_cable3.jpg) *License:* Public Domain *Contributors:* Baran Ivo

**File:STP-cable.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:STP-cable.svg> *License:* GNU Free Documentation License *Contributors:* Original: Uwe Schwöbel (de:Datei:STP-Kabel.png) English translation: Deelkar (File:STP-cable.png) Vector conversion: Sgalbertian

**Image:TwistedPair S-FTP.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:TwistedPair\\_S-FTP.jpg](http://en.wikipedia.org/w/index.php?title=File:TwistedPair_S-FTP.jpg) *License:* GNU Free Documentation License *Contributors:* Original uploader was Hurzelchen at de.wikipedia (Original text : Hurzelchen)

**File:S-UTP-cable.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:S-UTP-cable.svg> *License:* GNU Free Documentation License *Contributors:* Original: Uwe Schwöbel (de:Datei:SUTP-Kabel.png) English translation: Spinningspark (en:File:S-UTP-cable.png) Vector conversion: Sgalbertian

**File:S-STP-cable.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:S-STP-cable.svg> *License:* GNU Free Documentation License *Contributors:* Original: Uwe Schwöbel (de:Datei:SSTP-Kabel.png) English translation: Deelkar (en:File:S-STP-cable.png) Vector conversion: Sgalbertian

**File:fibreoptic.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Fibreoptic.jpg> *License:* GNU Free Documentation License *Contributors:* BigRiz

**File:Fiber optic illuminated.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Fiber\\_optic\\_illuminated.jpg](http://en.wikipedia.org/w/index.php?title=File:Fiber_optic_illuminated.jpg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Hustvedt

**File:Optical-fibre-junction-box.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Optical-fibre-junction-box.jpg> *License:* Public Domain *Contributors:* Alby (talk)

**File:Daniel Colladon's Lightfountain or Lightpipe, La Nature(magazine), 1884.JPG** *Source:* [http://en.wikipedia.org/w/index.php?title=File:DanielColladon's\\_Lightfountain\\_or\\_Lightpipe,LaNature\(magazine\),1884.JPG](http://en.wikipedia.org/w/index.php?title=File:DanielColladon's_Lightfountain_or_Lightpipe,LaNature(magazine),1884.JPG) *License:* Public Domain *Contributors:* -

**File:Flashflight red.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Flashflight\\_red.jpg](http://en.wikipedia.org/w/index.php?title=File:Flashflight_red.jpg) *License:* Public domain *Contributors:* Playhard, from the English Wikipedia

**File:OpticFiber.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:OpticFiber.jpg> *License:* Creative Commons Attribution 3.0 *Contributors:* Etan J. Tal

**File:Fiber-engineerguy.ogv** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Fiber-engineerguy.ogv> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Bill Hammack

**File:Optical-fibre.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Optical-fibre.svg> *License:* Public Domain *Contributors:* Gringer (talk)

**File:Laser in fibre.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Laser\\_in\\_fibre.jpg](http://en.wikipedia.org/w/index.php?title=File:Laser_in_fibre.jpg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Timwether

**File:Optical fiber types.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Optical\\_fiber\\_types.svg](http://en.wikipedia.org/w/index.php?title=File:Optical_fiber_types.svg) *License:* Creative Commons Attribution-Sharealike 3.0,2.5,2,0,1,0 *Contributors:* Mrzeon

**File:Singlemode fibre structure.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Singlemode\\_fibre\\_structure.svg](http://en.wikipedia.org/w/index.php?title=File:Singlemode_fibre_structure.svg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Original by Bob Mellish, SVG derivative by Benchill

**File:Zblan transmit.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Zblan\\_transmit.jpg](http://en.wikipedia.org/w/index.php?title=File:Zblan_transmit.jpg) *License:* Public Domain *Contributors:* NASA. Original uploader was Materialsscientist at en.wikipedia

**File:Reflection angles.svg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Reflection\\_angles.svg](http://en.wikipedia.org/w/index.php?title=File:Reflection_angles.svg) *License:* Creative Commons Attribution-ShareAlike 3.0 Unported *Contributors:* Arvelius, EDUCA33E, les

**File:Diffuse reflection.PNG** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Diffuse\\_reflection.PNG](http://en.wikipedia.org/w/index.php?title=File:Diffuse_reflection.PNG) *License:* GNU Free Documentation License *Contributors:* Original uploader was Theresa knott at en.wikipedia

**File:Phosphorus-pentoxide-3D-balls.png** *Source:* <http://en.wikipedia.org/w/index.php?title=File:Phosphorus-pentoxide-3D-balls.png> *License:* Public Domain *Contributors:* Benjah-bmm27, 2 anonymous edits

**File:OF-MCVD.svg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:OF-MCVD.svg> *License:* GNU Free Documentation License *Contributors:* User:User\_A1. Original uploader was User A1 at en.wikipedia

**File:Optical fiber cable.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:Optical\\_fiber\\_cable.jpg](http://en.wikipedia.org/w/index.php?title=File:Optical_fiber_cable.jpg) *License:* Creative Commons Attribution-Sharealike 3.0,2,5,2,0,1,0 *Contributors:* Buy\_on\_turbosquid\_optical.jpg: Cable master derivative work: Srleffler (talk)

**File:ST-optical-fiber-connector-hdr-0a.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:ST-optical-fiber-connector-hdr-0a.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Adamantios

**File:DShaped1.png** *Source:* <http://en.wikipedia.org/w/index.php?title=File:DShaped1.png> *License:* GNU Free Documentation License *Contributors:* User:Domitor

**File:MMF optical.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:MMF\\_optical.jpg](http://en.wikipedia.org/w/index.php?title=File:MMF_optical.jpg) *License:* Public Domain *Contributors:* Original uploader was Timewalk at en.wikibooks

**file:FC-optical-fiber-connector-hdr-0a.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:FC-optical-fiber-connector-hdr-0a.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Adamantios

**File:E2000-Connector.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:E2000-Connector.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Kirnehkrib

**File:ESCON connector.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:ESCON\\_connector.jpg](http://en.wikipedia.org/w/index.php?title=File:ESCON_connector.jpg) *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Kirnehkrib

**file:LC-optical-fiber-connector-hdr-0a.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:LC-optical-fiber-connector-hdr-0a.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Adamantios

**file:FOLuxCis01.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:FOLuxCis01.jpg> *License:* Public Domain *Contributors:* 12Gooner89, Srleffler

**file:FDDI-optical-fiber-connector-hdr-0a.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:FDDI-optical-fiber-connector-hdr-0a.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Adamantios

**File:MTP-Connector.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:MTP-Connector.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Kirnehkrib

**file:MTRJ-optical-fiber-connector-hdr-0a.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:MTRJ-optical-fiber-connector-hdr-0a.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Adamantios

**file:DSCF0058.JPG** *Source:* <http://en.wikipedia.org/w/index.php?title=File:DSCF0058.JPG> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* AleiPhoenix

**file:SC-optical-fiber-connector-hdr-0a.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:SC-optical-fiber-connector-hdr-0a.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Adamantios

**File:FSMA.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:FSMA.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* User:Kirnehkrib

**file:ST-optical-fiber-connector-hdr-0a.jpg** *Source:* <http://en.wikipedia.org/w/index.php?title=File:ST-optical-fiber-connector-hdr-0a.jpg> *License:* Creative Commons Attribution-Sharealike 3.0 *Contributors:* Adamantios

**file:TOS LINK clear cable.jpg** *Source:* [http://en.wikipedia.org/w/index.php?title=File:TOS\\_LINK\\_clear\\_cable.jpg](http://en.wikipedia.org/w/index.php?title=File:TOS_LINK_clear_cable.jpg) *License:* GNU Free Documentation License *Contributors:* Hustvedt

# License

---

Creative Commons Attribution-Share Alike 3.0 Unported  
[//creativecommons.org/licenses/by-sa/3.0/](http://creativecommons.org/licenses/by-sa/3.0/)