COMPUTER NETWORKS

INDEX

PROJECT BY:

SANIL S. SINAI BORKAR

TE COMP

ROLL NO : 060536

Assignment 1: **Study of different Networking an Internetworking Components**

A **computer network** is a group of interconnected computers. Networks may be classified according to a wide variety of characteristics. This article provides a general overview of some types and categories and also presents the basic components of a network.

A network is a collection of computers and devices connected to each other. The network allows computers to communicate with each other and share resources and information. The Advance Research Projects Agency (ARPA) designed "Advanced Research Projects Agency Network" (ARPANET) for the United States Department of Defense. It was the first computer network in the world in late 1960's and early 1970's.

Network classification

The following list presents categories used for classifying networks.

Computer networks can also be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as Optical fiber, Ethernet, Wireless LAN, HomePNA, or Power line communication.

Ethernet uses physical wiring to connect devices. Frequently deployed devices include hubs, switches, bridges and/or routers.

Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium.

1)Scale

Based on their scale, networks can be classified as Local Area Network (LAN), Wide Area Network (WAN), Metropolitan Area Network (MAN), Personal Area Network (PAN), Virtual Private Network (VPN), Campus Area Network (CAN), Storage Area Network (SAN), etc.

2)Functional relationship (network architecture)

Computer networks may be classified according to the functional relationships which exist among the elements of the network, e.g., Active Networking, Client-server and Peer-to-peer (workgroup) architecture.

3)Network topology

Computer networks may be classified according to the network topology upon which the network is based, such as bus network, star network, ring network, mesh network, star-bus network, tree or hierarchical topology network. Network topology signifies the way in which devices in the network see their logical relations to one another. The use of the term "logical" here is significant. That is, network topology is independent of the "physical" layout of the network. Even if networked computers are physically placed in a

linear arrangement, if they are connected via a hub, the network has a Star topology, rather than a bus topology. In this regard the visual and operational characteristics of a network are distinct; the logical network topology is not necessarily the same as the physical layout. Networks may be classified based on the method of data used to convey the data, these include digital and analog networks.

Basic hardware components

All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers. In addition, some method of connecting these building blocks is required, usually in the form of galvanic cable (most commonly Category 5 cable). Less common are microwave links (as in IEEE 802.12) or optical cable ("optical fiber"). An ethernet card may also be required.

1)Network interface cards

A **network card**, **network adapter**, **network interface controller** (**NIC**), **network interface card**, or **LAN adapter** is a computer hardware component designed to allow computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly. The NIC provides the transfer of data in megabytes.

Although other network technologies exist, Ethernet has achieved near-ubiquity since the mid-1990s Wendy WU. Every Ethernet network card has a unique 48-bit serial number called a MAC address, which is stored in ROM carried on the card. Every computer on an Ethernet network must have a card with a unique MAC address. Normally it is safe to assume that no two network cards will share the same address, because card vendors purchase blocks of addresses from the Institute of Electrical and Electronics Engineers (IEEE) and assign a unique address to each card at the time of manufacture.

Whereas network cards used to be expansion cards that plug into a computer bus, the low cost and ubiquity of the Ethernet standard means that most newer computers have a network interface built into the motherboard. These either have Ethernet capabilities integrated into the motherboard chipset or implemented via a low cost dedicated Ethernet

chip, connected through the PCI (or the newer PCI express bus). A separate network card is not required unless multiple interfaces are needed or some other type of network is used. Newer motherboards may even have dual network (Ethernet) interfaces built-in.

The card implements the electronic circuitry required to communicate using a specific physical layer and data link layer standard such as Ethernet or token ring. This provides a base for a full network protocol stack, allowing communication among small groups of computers on the same LAN and large-scale network communications through routable protocols, such as IP.

1) Wired Network Interface Card (NIC) is a hardware interface that handles and allows a network capable device access to a computer network such as the internet. The NIC has a ROM chip that has a unique Media Access Control (MAC) Address burned into it. The MAC address identifies the vendor MAC address which identifies it on the LAN. The NIC exists on both the ' Physical Layer' (Layer 1) and the 'Data Link Layer' (Layer 2) of the OSI model.

Sometimes the word 'controller' and 'card' is used interchangeably when talking about networking because the most common NIC is the Network Interface Card. Although 'card' is more commonly used, it is less encompassing. The 'controller' may take the form of a network card that is installed inside a computer, or it may refer to an embedded component as part of a computer motherboard, a router, expansion card, printer interface, or a USB device.

A MAC Address is a 48 bit network hardware identifier that is burned into a ROM chip on the NIC to identify that device on the network. The first 24 bits is called the Organizationally Unique Identifier (OUI) and is largely manufacturer dependent. Each OUI allows for 16,777,216 Unique NIC Addresses.

Smaller manufacturers that do not have a need for over 4096 unique NIC addresses may opt to purchase an Individual Address Block (IAB) instead. An IAB consists of the 24 bit OUI, plus a 12 bit extension (taken from the 'potential' NIC portion of the MAC address)

There are four techniques used to transfer data, the NIC may use one or more of these techniques.

- **Polling** is where the microprocessor examines the status of the peripheral under program control.
- **Programmed I/O** is where the microprocessor alerts the designated peripheral by applying its address to the system's address bus.
- **Interrupt-driven I/O** is where the peripheral alerts the microprocessor that it's ready to transfer data.
- **DMA** is where the intelligent peripheral assumes control of the system bus to access memory directly. This removes load from the CPU but requires a separate processor on the card.

A network card typically has a twisted pair, BNC, or AUI socket where the network cable is connected, and a few LEDs to inform the user of whether the network is active, and whether or not there is data being transmitted on it. Network Cards are typically available in 10/100/1000 Mbit/s varieties. This means they can support a transfer rate of 10, 100 or 1000 Megabits per second.

2) Wireless network interface card

(a)

(a)A wireless network interface device with a USB interface and internal antenna.

A **wireless network interface controller** (WNIC) is a network card which connects to a radio-based computer network, unlike a regular network interface controller (NIC) which connects to a wire-based network such as token ring or ethernet. A WNIC, just like a NIC, works on the Layer 1 and Layer 2 of the OSI Model. A WNIC is an essential component for wireless desktop computer. This card uses an antenna to communicate through microwaves. A WNIC in a desktop computer usually is connected using the PCI bus. Other connectivity options are USB and PC card. Integrated WNIC's are also available, (typically in Mini PCI/PCI Express Mini Card form).

Modes of operation

A WNIC can operate in two modes known as **infrastructure mode** and **ad hoc mode**.

In an infrastructure mode network the WNIC needs an access point: all data is transferred using the access point as the central hub. All wireless nodes in an infrastructure mode network connect to an access point. All nodes connecting to the access point must have the same service set identifier (SSID) as the access point, and if the access point is enabled with WEP they must have the same WEP key or other authentication parameters.

In an ad-hoc mode network the WNIC does not require an access point, but rather can directly interface with all other wireless nodes directly. All the nodes in an ad-hoc network must have the same channel and SSID.

Specifications commonly used in marketing materials for WNICs include:

- Wireless data transfer rates (measured in Mbit/s); these range from 2 Mbit/s to 54 Mbit/s.[1]
- Wireless transmit power (measured in dBm)
- Wireless network standards (may include standards such as 802.11b, 802.11g, 802.11n, etc.) 802.11g offers data transfer speeds equivalent to 802.11a – up to 54 Mbit/s – and the wider 300-foot (91 m) range of 802.11b, and is backward compatible with 802.11b.

Wireless local area network standards

802.11 Protocol	Release[2]	Freq. (GHz)	Typ throughput (Mbit/s) [*citation needed*]	Max net bitrate (Mbit/s)	Modulation	$r_{in.}$ (m)	$r_{out.}$ (m)
–	Jun 1997	2.4	00.9	002	IR/FH/DSSS	~20	~100
a	Sep 1999	5	23	054	OFDM	~35	~120
b	Sep 1999	2.4	04.3	011	DSSS	~38	~140
g	Jun 2003	2.4	19	054	OFDM	~38	~140
n	~ Jun 2010	2.4 5	74	300	OFDM	~70	~250[3]
y	Nov 2008	3.7	23	054	OFDM	~50	~5000

2)Repeaters

A **repeater** is an electronic device that receives a signal 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 runs longer than 100 meters away from the computer.

The term "repeater" originated with telegraphy and referred to an electromechanical device used to regenerate telegraph signals. Use of the term has continued in telephony and data communications.

In telecommunication, the term **repeater** has the following standardized meanings:

1. An analog device that amplifies an input signal regardless of its nature (analog or digital).
2. A digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission.

Because repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they operate on the Physical layer, the first layer of the OSI model.

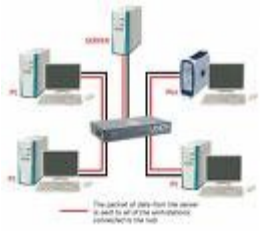
3)Hubs

A **network hub** or **repeater hub** is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and thus making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is thus a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

A hub contains multiple ports. When a packet arrives at one port, it is copied unmodified to all ports of the hub for transmission. The destination address in the frame is not changed to a broadcast address.

Hubs also often come with a BNC and/or AUI connector to allow connection to legacy 10BASE2 or 10BASE5 network segments. The availability of low-priced network switches has largely rendered hubs obsolete but they are still seen in older installations and more specialized applications.

A **hub** is an element of hardware for centralising network traffic coming from multiple hosts, and to propagate the signal. The hub has a certain number of ports (it has enough ports to link machines to one another, usually 4, 8, 16 or 32). Its only goal is to recover binary data coming into a port and send it to all the other ports. As with a repeater, a hub operates on layer 1 of the OSI model, which is why it is sometimes called a ***multiport repeater*.**



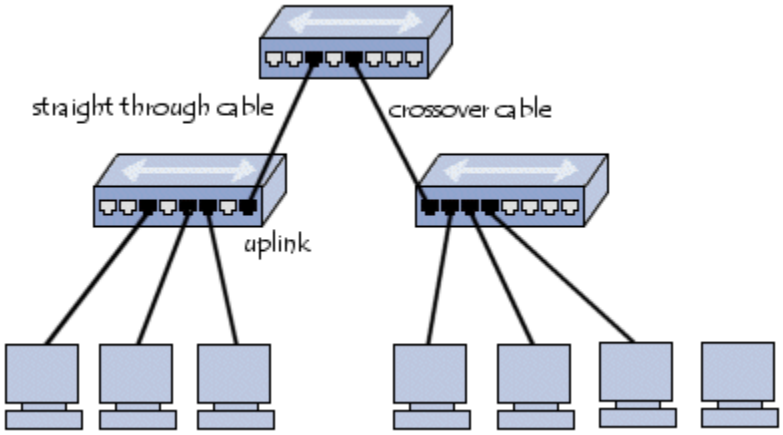

The hub connects several machines together, sometimes arranged in a star shape, which gives it its name, due to the fact that all communication coming from the machines on the network passes through it.

Types of hubs

- "**Active**" hubs: They are connected to an electrical power source and are used to refresh the signal being sent to the ports.
- "**Passive**" ports: They simply send the signal to all the connected hosts, without amplifying it.

Connecting multiple hubs

It is possible to connect several hubs together in order to centralise a larger number of machines; this is sometimes called a *daisy chain*. To do this, all that is needed is to connect the hubs using crossover cable, a kind of cable which links the in/out ports on one end to those on the other.
Hubs generally have a special port called an "*uplink*" for connecting two hubs together using a patch cable. There are also hubs which can cross or uncross their ports automatically depending on whether they are connected to a host or a hub.



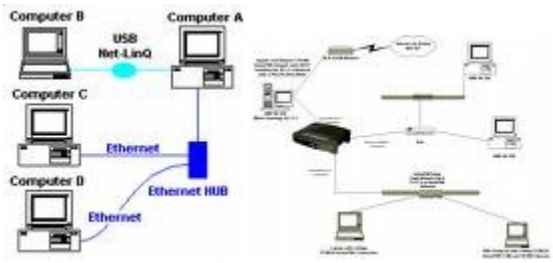
One of the most commonly used networking hardware devices are hubs. However, the inexpensive switch is rapidly replacing the hub. Anyway, hubs serve as central connection points for local area networks (LANs) that typically embrace the star topology.

The basic hub contains no active electronics and cannot be used to extend a LAN past its cabling distance specifications. Yet, hubs organize your cables and relay data signals to all computers that exist on your LAN.

Hubs are used on networks where twisted-pair cabling is used. The ports, which are available on the hub, provide connection points for the devices on the network. Computers and devices are connected to the hub via network cables to individual ports. In cases where a LAN outgrows the size of its hub, a new hub can be attached by daisy-chaining them together using a short connection cable, which is often referred to as a rattail.

Hubs come in many different shapes and sizes and are available in a wide range of prices. The more ports available on the hub, the more expensive the hub. Also, hubs that support faster varieties of Ethernet, for example Fast Ethernet, will also cost more.

4) Network Bridges



A **network bridge** connects multiple network segments at the data link layer (layer 2) of the OSI model. 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 only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received.

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:

1. **Local bridges**: Directly connect local area networks (LANs)

2. **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 by routers.
3. **Wireless bridges**: Can be used to join LANs or connect remote stations to LANs.

5)Network Switches


A switch is a device that forwards and filters OSI layer 2 datagrams (chunk of data communication) between ports (connected cables) based on the MAC addresses in the packets.[3] This is distinct from a hub in that it only forwards the packets to the ports involved in the communications rather than all ports connected. Strictly speaking, a switch is not capable of routing traffic based on IP address (OSI Layer 3) which is necessary for communicating between network segments or within a large or complex LAN. Some switches are capable of routing based on IP addresses but are still called switches as a marketing term. A switch normally has numerous ports, with the intention being that most or all of the network is connected directly to the switch, or another switch that is in turn connected to a switch.

Switch is a marketing term that encompasses routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier). Switches may operate at one or more OSI model layers, including physical, data link, network, or transport (i.e., end-to-end). A device that operates simultaneously at more than one of these layers is called a multilayer switch.

Overemphasizing the ill-defined term "switch" often leads to confusion when first trying to understand networking. Many experienced network designers and operators recommend starting with the logic of devices dealing with only one protocol level, not all of which are covered by OSI. Multilayer device selection is an advanced topic that may lead to selecting particular implementations, but multilayer switching is simply not a real-world design concept.

A **network switch** is a computer networking device that connects network segments.

The term commonly refers to a Network bridge that processes and routes data at the Data link layer (layer 2) of the OSI model. Switches that additionally process data at the Network layer (layer 3 and above) are often referred to as Layer 3 switches or Multilayer switches.

Functions of a Network Switch

As with hubs, Ethernet implementations of network switches support either 10/100 Mbit/s or 10/100/1000 Mbit/s ports Ethernet standards. Large switches may have 10 Gbit/s ports. Switches differ from hubs in that they can have ports of different speed.

The *network switch*, *packet switch* (or just *switch*) plays an integral part in most Ethernet local area networks or *LANs*. Mid-to-large sized LANs contain a number of linked managed switches. Small office, home office (SOHO) applications typically use a single switch, or an all-purpose converged device such as gateway access to small office/home office broadband services such as DSL router or cable, Wi-Fi router. In most of these cases, the end user device contains a router and components that interface to the particular physical broadband technology, as in the Linksys 8-port and 48-port devices. User devices may also include a telephone interface to VoIP.

In the context of a standard 10/100 Ethernet switch, a switch operates at the data-link layer of the OSI model to create a different collision domain per switch port. If you have 4 computers A/B/C/D on 4 switch ports, then A and B can transfer data between them as well as C and D at the same time, and they will never interfere with each others' conversations. In the case of a "hub" then they would all have to share the bandwidth, run in half-duplex and there would be collisions and retransmissions. Using a switch is called micro-segmentation. It allows you to have dedicated bandwidth on point to point connections with every computer and to therefore run in full duplex with no collisions.

Role of switches in networks

Network switch is a marketing term rather than a technical one. Switches may operate at one or more OSI layers, including physical, data link, network, or transport (i.e., end-to-end). A device that operates simultaneously at more than one of these layers is called a multilayer switch, although use of the term is diminishing.

In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, for example Ethernet, Fibre Channel, ATM, and 802.11. This connectivity can be at any of the layers mentioned. While Layer 2 functionality is adequate for speed-shifting within one technology, interconnecting technologies such as Ethernet and token ring are easier at Layer 3.

Interconnection of different Layer 3 networks is done by routers. If there are any features that characterize "Layer-3 switches" as opposed to general-purpose routers, it tends to be that they are optimized, in larger switches, for high-density Ethernet connectivity.

In some service provider and other environments where there is a need for much analysis of network performance and security, switches may be connected between WAN routers as places for analytic modules. Some vendors provide firewall,[2][3] network intrusion detection,[4] and performance analysis modules that can plug into switch ports. Some of these functions may be on combined modules.[5]

In other cases, the switch is used to create a mirror image of data that can go to an external device. Since most switch port mirroring provides only one mirrored stream, network hubs can be useful for fanning out data to several read-only analyzers, such as intrusion detection systems and packet sniffers.

Types of switches

Form factor

- Desktop, not mounted in an enclosure, typically intended to be used in a home or office environment outside of a wiring closet
- Rack mounted
- Chassis — with swappable "switch module" cards. e.g. Alcatel's OmniSwitch 7000; Cisco Catalyst switch 4500 and 6500; 3Com 7700, 7900E, 8800.

Configuration options

- ***Unmanaged* switches** — These switches have no configuration interface or options. They are plug-and-play. They are typically the least expensive switches, found in home, SOHO, or small businesses. They can be desktop or rack mounted.
- ***Managed* switches** — These switches have one or more ways, or interfaces, to modify the operation of the switch. Common management methods include: a serial console or Command Line Interface accessed via telnet or Secure Shell; an embedded Simple Network Management Protocol SNMP agent allowing management from a remote console or management station; a web interface for management from a web browser. Examples of configuration changes that one can do from a managed switch include: enable features such as Spanning Tree Protocol; set port speed; create or modify VLANs, etc. Two sub-classes of managed switches are marketed today:
    - ***Smart* (or intelligent) switches** — These are managed switches with a limited set of management features. Likewise "web-managed" switches are switches which fall in a market niche between unmanaged and managed. For a price much lower than a fully managed switch they provide a web interface (and usually no CLI access) and allow configuration of basic settings, such as VLANs, port-speed and duplex.[9]
    - ***Enterprise Managed* (or fully managed) switches** - These have a full set of management features, including Command Line Interface, SNMP agent, and web interface. They may have additional features to manipulate configurations, such as the ability to display, modify, backup and restore configurations. Compared with smart switches, enterprise switches have more features that can be customized or optimized, and are generally more expensive than "smart" switches. Enterprise switches are typically found in networks with larger number of switches and connections, where centralized management is a significant savings in administrative time and effort. A Stackable switch is a version of enterprise-managed switch.

6) Routers

A **router** (pronounced /'rautər/ in the USA and Canada, pronounced /'ru:tə/ in the UK and Ireland, or either pronunciation in Australia) is a networking device whose software and hardware are usually tailored to the tasks of routing and forwarding information. For example, on the Internet, information is directed to various paths by routers.

Routers connect two or more logical subnets, which do not necessarily map one-to-one to the physical interfaces of the router.[1] The term "layer 3 switch" often is used interchangeably with router, but switch is a general term without a rigorous technical definition. In marketing usage, it is generally optimized for Ethernet LAN interfaces and may not have other physical interface types. In comparison, a network hub does not do any routing, instead every packet it receives on one network line gets forwarded to all the other network lines. Routers are networking devices that forward data packets between networks using headers and forwarding tables to determine the best path to forward the packets. Routers work at the network layer .

Cisco 1800 Router

Nortel ERS 8600

Cisco 7600 Routers

Routers operate in two different planes :

- **Control plane,** in which the router learns the outgoing interface that is most appropriate for forwarding specific packets to specific destinations,
- **Forwarding plane**, which is responsible for the actual process of sending a packet received on a logical interface to an outbound logical interface.

Routers generally contain a specialized operating system (e.g. Cisco's IOS or Juniper Networks JUNOS and JUNOSe or Extreme Networks XOS[3]), RAM, NVRAM, flash memory, and one or more processors, as well as two or more network interfaces. Except for multiple network interfaces this is typical of an embedded computer.

High-end routers contain many processors and specialized Application-specific integrated circuits (ASICs) and do a great deal of parallel processing. Chassis based systems like the

Nortel MERS-8600 or ERS-8600 routing switch, (pictured right) have multiple ASICs on every module and allow for a wide variety of LAN, MAN, METRO, and WAN technology ports or other, customizable connections. Simpler routers are used where cost is more important and traffic is less, for example, in providing a home Internet service. With the appropriate software (such as Untangle, SmoothWall, XORP or Quagga), an ordinary personal computer can become a router.

Control plane

Routers are like intersections whereas switches are like streets.

Control plane processing leads to the construction of what is variously called a routing table or routing information base (RIB). The RIB may be used by the Forwarding Plane to look up the outbound interface for a given packet, or, depending on the router implementation, the Control Plane may populate a separate forwarding information base (FIB) with destination information. RIBs are optimized for efficient updating with control mechanisms such as routing protocols, while FIBs are optimized for the fastest possible lookup of the information needed to select the outbound interface.

The Control Plane constructs the routing table from knowledge of the up/down status of its local interfaces, from hard-coded static routes, and from exchanging routing protocol information with other routers. It is not compulsory for a router to use routing protocols to function, if for example it was configured solely with static routes. The routing table stores the best routes to certain network destinations, the "routing metrics" [ex:time delay,distance,queue length] associated with those routes, and the path to the next hop router.

Routers do maintain state on the routes in the RIB/routing table, but this is quite distinct from not maintaining state on individual packets that have been forwarded.

Forwarding plane (a.k.a. data plane)

For the pure Internet Protocol (IP) forwarding function, router design tries to minimize the state information kept on individual packets. Once a packet is forwarded, the router should no longer retain statistical information about it. It is the sending and receiving endpoints that keeps information about such things as errored or missing packets.

Forwarding decisions can involve decisions at layers other than the IP internetwork layer or OSI layer 3. Again, the marketing term switch can be applied to devices that have these capabilities. A function that forwards based on data link layer, or OSI layer 2, information, is properly called a bridge. Marketing literature may call it a layer 2 switch, but a switch has no precise definition.

Among the most important forwarding decisions is deciding what to do when congestion occurs, i.e., packets arrive at the router at a rate higher than the router can process. Three policies commonly used in the Internet are Tail drop, Random early detection, and

Weighted random early detection. Tail drop is the simplest and most easily implemented; the router simply drops packets once the length of the queue exceeds the size of the buffers in the router. Random early detection (RED) probabilistically drops datagrams early when the queue exceeds a configured size. Weighted random early detection requires a weighted average queue size to exceed the configured size, so that short bursts will not trigger random drops.

Types of routers

Routers may provide connectivity inside enterprises, between enterprises and the Internet, and inside Internet Service Providers (ISP). The largest routers (for example the Cisco CRS-1 or Juniper T1600) interconnect ISPs, are used inside ISPs, or may be used in very large enterprise networks. The smallest routers provide connectivity for small and home offices.

1)Routers for Internet connectivity and internal use

Routers intended for ISP and major enterprise connectivity will almost invariably exchange routing information with the Border Gateway Protocol. RFC 4098[4] defines several types of BGP-speaking routers:

- **Provider Edge Router**: Placed at the edge of an ISP network, it speaks external BGP (eBGP) to a BGP speaker in another provider or large enterprise Autonomous System (AS).
- **Subscriber Edge Router**: Located at the edge of the subscriber's network, it speaks eBGP to its provider's AS(s). It belongs to an end user (enterprise) organization.
- **Inter-provider Border Router**: Interconnecting ISPs, this is a BGP speaking router that maintains BGP sessions with other BGP speaking routers in other providers' ASes.
- **Core router**: A router that resides within the middle or backbone of the LAN network rather than at its periphery.

  Within an ISP: Internal to the provider's AS, such a router speaks internal BGP (iBGP) to that provider's edge routers, other intra-provider core routers, or the provider's inter-provider border routers.
  "Internet backbone:" The Internet does not have a clearly identifiable backbone, as did its predecessors. See default-free zone (DFZ). Nevertheless, it is the major ISPs' routers that make up what many would consider the core. These ISPs operate all four types of the BGP-speaking routers described here. In ISP usage, a "core" router is internal to an ISP, and used to interconnect its edge and border routers. Core routers may also have specialized functions in virtual private networks based on a combination of BGP and Multi-Protocol Label Switching (MPLS)[5].

Router's are also used for port fowarding for private servers.

2)Small Office Home Office (SOHO) connectivity

Residential gateways (often called routers) are frequently used in homes to connect to a broadband service, such as IP over cable or DSL. A home router may allow connectivity to an enterprise via a secure Virtual Private Network.

While functionally similar to routers, residential gateways use port address translation in addition to routing. Instead of connecting local computers to the remote network directly, a residential gateway makes multiple local computers appear to be a single computer.

3)Enterprise routers

All sizes of routers may be found inside enterprises. The most powerful routers tend to be found in ISPs but academic and research facilities. Large businesses may also need powerful routers.

A three-layer model is in common use, not all of which need be present in smaller networks [6].

Distribution

Distribution routers aggregate traffic from multiple access routers, either at the same site, or to collect the data streams from multiple sites to a major enterprise location. Distribution routers often are responsible for enforcing quality of service across a WAN, so they may have considerable memory, multiple WAN interfaces, and substantial processing intelligence.

They may also provide connectivity to groups of servers or to external networks. In the latter application, the router's functionality must be carefully considered as part of the overall security architecture. Separate from the router may be a Firewall or VPN concentrator, or the router may include these and other security functions.

When an enterprise is primarily on one campus, there may not be a distinct distribution tier, other than perhaps off-campus access. In such cases, the access routers, connected to LANs, interconnect via core routers.

7)Access Point

(a) (b)

(a) Linksys WAP54G 802.11g Wireless Access Point
(b) OSBRiDGE 3GN - 802.11n Access Point and UMTS/GSM Gateway in one device

In computer networking, a **wireless access point** (**WAP** or **AP**) is a device that allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a wired network, and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.

Prior to wireless networks, setting up a computer network in a business, home, or school often required running many cables through walls and ceilings in order to deliver network access to all of the network-enabled devices in the building. With the advent of the Wireless Access Point, network users are now able to add devices that access the network with few or no new cables. Today's WAPs are built to support a standard for sending and receiving data using radio frequencies rather than cabling. Those standards, and the frequencies they use are defined by the IEEE. Most WAPs use IEEE 802.11 standards.

Common WAP Applications

A typical corporate use involves attaching several WAPs to a wired network and then providing wireless access to the office LAN. Within the range of the WAPs, the wireless end user has a full network connection with the benefit of mobility. In this instance, the WAP functions as a gateway for clients to access the wired network.

A Hot Spot is a common public application of WAPs, where wireless clients can connect to the Internet without regard for the particular networks to which they have attached for the moment. The concept has become common in large cities, where a combination of coffeehouses, libraries, as well as privately owned open access points, allow clients to stay more or less continuously connected to the Internet, while moving around. A collection of connected Hot Spots can be referred to as a *lily-pad network*.

The majority of WAPs are used in Home wireless networks.[*citation needed*] Home networks generally have only one WAP to connect all the computers in a home. Most are wireless routers, meaning converged devices that include a WAP, router, and often an ethernet switch in the same device. Many also converge a broadband modem. In places where most homes have their own WAP within range of the neighbors' WAP, it's possible for technically savvy people to turn off their encryption and set up a wireless community network, creating an intra-city communication network without the need of wired networks.

A WAP may also act as the network's arbitrator, negotiating when each nearby client device can transmit. However, the vast majority of currently installed IEEE 802.11 networks do not implement this, using a distributed pseudo-random algorithm called CSMA/CD instead.

Limitations

One IEEE 802.11 WAP can typically communicate with 30 client systems located within a radius of 100 m.[citation needed] However, the actual range of communication can vary significantly, depending on such variables as indoor or outdoor placement, height above ground, nearby obstructions, other electronic devices that might actively interfere with the signal by broadcasting on the same frequency, type of antenna, the current weather, operating radio frequency, and the power output of devices. Network designers can extend the range of WAPs through the use of repeaters and reflectors, which can bounce or amplify radio signals that ordinarily would go un-received. In experimental conditions, wireless networking has operated over distances of several kilometers.

Most jurisdictions have only a limited number of frequencies legally available for use by wireless networks. Usually, adjacent WAPs will use different frequencies to communicate with their clients in order to avoid interference between the two nearby systems. Wireless devices can "listen" for data traffic on other frequencies, and can rapidly switch from one frequency to another to achieve better reception. However, the limited number of frequencies becomes problematic in crowded downtown areas with tall buildings using multiple WAPs. In such an environment, signal overlap becomes an issue causing interference, which results in signal dropage and data errors.

Wireless networking lags behind wired networking in terms of increasing bandwidth and throughput. While (as of 2004) typical wireless devices for the consumer market can reach speeds of 11 Mbit/s (megabits per second) (IEEE 802.11b) or 54 Mbit/s (IEEE 802.11a, IEEE 802.11g), wired hardware of similar cost reaches 1000 Mbit/s (Gigabit Ethernet). One impediment to increasing the speed of wireless communications comes from Wi-Fi's use of a shared communications medium, so a WAP is only able to use somewhat less than half the actual over-the-air rate for data throughput. Thus a typical 54 MBit/s wireless connection actually carries TCP/IP data at 20 to 25 Mbit/s. Users of legacy wired networks expect faster speeds, and people using wireless connections keenly want to see the wireless networks catch up.

As of 2007 a new standard for wireless, 802.11n is awaiting final certification from IEEE. This new standard operates at speeds up to 540 Mbit/s and at longer distances (~50 m) than 802.11g. Use of legacy wired networks (especially in consumer applications) is expected[by whom?] to decline sharply as the common 100 Mbit/s speed is surpassed and users no longer need to worry about running wires to attain high bandwidth.[citation needed]

By the year 2008 *draft* 802.11n based access points and client devices have already taken a fair share of the market place but with inherent problems integrating products from different vendors.

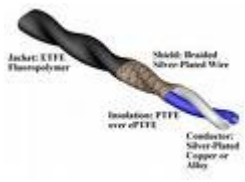
8)Transmission Media

1)Magnetic Media



Disks and tapes are one of the most popular methods of transmitting data from one computer to another fast. The problem is that the source and destination have to be very close together for this to be reasonable. If you need to transmit your data to another town in less time than it would take to drive there, then another method of transfer will be needed.

2) Twisted Pair



Twisted Pair wiring (Cat 3 and Cat 5) are popular methods of transferring data. They are especially prevalent in the LAN environment. The twists allow the signal to travel further than it could on a regular copper wire. The more twists per centimeter, the further the signal can travel. This is why Cat 5 wire (with more twists) is preferred over Cat 3 wire. Twisted pair wires consist of two strands of copper twisted together; the wires are unshielded, which is why Twisted Pair wire is also called Unshielded Twisted Pair (UTP). Twisted pair cabling is a form of wiring in which two conductors (the forward and return 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. [edit] Unshielded twisted pair (UTP)

Unshielded twisted pair

Twisted pair cables were first used in telephone systems by Alexander Graham Bell in 1881. By 1900, the entire American telephone line network was either twisted pair or open wire with similar arrangements 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.

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.

UTP cable is also the most common cable used in computer networking. UTP cables are often called ethernet cables after Ethernet, the most common data networking standard that 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 middle to high-end cameras include a UTP output with setscrew terminals. This is made possible by the fact that UTP cable bandwidth has improved to match the baseband of television signals. While the video recorder most likely still has unbalanced BNC connectors for standard coaxial cable, a balun is used to convert from 100-ohm balanced UTP to 75-ohm unbalanced. A balun can also be used at the camera end for ones without a UTP output. Only one pair is necessary for each video signal.

Twisted pair cables are often shielded in 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. The shielding must be grounded for the shielding to work.

1)Screened unshielded twisted pair (S/UTP)

Also known as Fully shielded[*citation needed*] (or Foiled) Twisted Pair (FTP), is a screened UTP cable (ScTP).

2)Shielded twisted pair (STP or STP-A)

STP cabling includes metal shielding over each individual pair of copper wires. This type of shielding protects cable from external EMI (electromagnetic interferences). e.g. the 150 ohm shielded twisted pair cables defined by the IBM Cabling System specifications and used with token ring networks.

3)Screened shielded twisted pair (S/STP or S/FTP)

S/STP cabling, also known as Screened Fully shielded Twisted Pair (S/FTP), [1] 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*[1].

Advantages

- It is a thin, flexible cable that is easy to string between walls.
- Because UTP is small, it does not quickly fill up wiring ducts.
- UTP costs less per foot than any other type of LAN cable.

Disadvantages

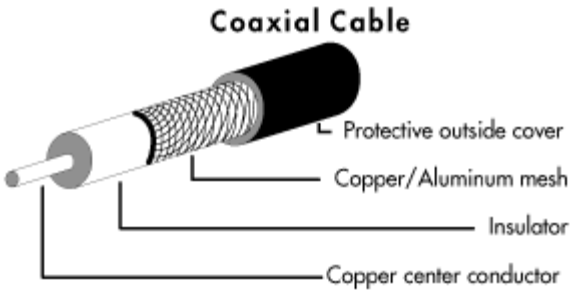
- Twisted pair's susceptibility to the electromagnetic interference greatly depends on the pair twisting schemes (usually patented by the manufacturers) staying intact during the installation. As a result, twisted pair cables usually have stringent requirements for maximum pulling tension as well as minimum bend radius. This relative fragility of twisted pair cables makes the installation practices an important part of ensuring the cable's performance.

3)Coxial Cables

Coaxial cable is a cable consisting of an inner conductor, surrounded by a tubular insulating layer typically made from a flexible material with a high **dielectric constant**, all of which is then surrounded by another conductive layer (typically of fine woven wire for flexibility, or of a thin metallic foil), and then finally covered again with a thin insulating layer on the outside. The term **coaxial** comes from the inner conductor and the outer shield sharing the same geometric axis. Coaxial cables are often used as a **transmission line** for **radio frequency** signals. In a hypothetical ideal coaxial cable the **electromagnetic field** carrying the signal exists only in the space between the inner and outer **conductors**. Practical cables achieve this objective to a high degree. A coaxial cable provides protection of signals from external electromagnetic interference, and effectively guides signals with low emission along the length of the cable

a) Baseband Coaxial Cable

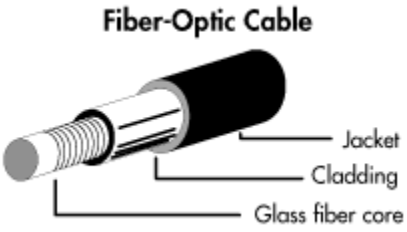
Reading through this material is relatively easy. It describes the technical details of coaxial cable, which is an insulated copper wire covered with a mesh conductor, with a coating of plastic on top of that. The reason it is made like that is to provide a combination of high bandwidth with low noise. Although it has been replaced by fiber optics in the long-distance telephone industry, the cable industry still uses coaxial cable.



b)Broadband Coaxial Cable

In networking, the term "broadband" refers to any cable that uses analog transmission. The reason broadband cables are used is to get longer distances, but amplifiers are needed. These amplifiers transform the cable into a unidirectional cable. If two-way communication is needed, two cables will be needed (one going one way, the other goes the other way).

4) Fiber Optics

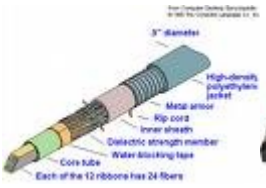


Although computing technology is rapidly advancing, it is not gaining ground nearly as fast as communication technology is. Fiber optics is one of the advances that has propelled communication technology into the future at high speeds. Communication over fiber optics requires a source (of light), a line (transmission medium = fiber), and a destination (to detect the light). The light stays within the fiber line because of the angle at which the light hits the surface of the fiber line. Instead of passing through the fiber's surface (like a window), the light bounces off of it (like a mirror). The light propagates down the fiber line because it continually reflects off the surface from the inside; the light never escapes the fiber line until the receiver detects it.

Like copper, fiber optics suffers problems when transmitting over a distance. Attenuation (a weakening of the power of a signal) occurs, as well as dispersion (the spreading out of light waves over a distance). The discovery of solitons has helped wipe out the problem of dispersion, though. A fiber cable is heavily insulated like coax, but it has several differences. The core of the cable is a glass strand, which is surrounded by a thick glass covering, which is then covered by plastic.

When compared to copper for its overall purposes, fiber wins because it is lighter, higher bandwidth, easier to install, harder to tap, and the signal stays stronger longer than in copper. The only drawback to fiber at this point in time is the lack of familiarity among the engineering community with the fiber technology compared to the copper.

Optical fiber cables are shown in the figure



An **optical fiber** (or **fibre**) is a glass or plastic fiber that carries light along its length. **Fiber optics** is the overlap of applied science and engineering concerned with the design and application of optical fibers. 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 communications. Fibers are used instead of metal wires because signals travel along them with less loss, and they are also immune to electromagnetic interference. Fibers are also used for illumination, and are wrapped in bundles so they can be used to carry images, thus allowing viewing in tight spaces. Specially designed fibers are used for a variety of other applications, including sensors and fiber lasers.

Light is kept in the core of the optical fiber by total internal reflection. This causes the fiber to act as a waveguide. Fibers which support many propagation paths or transverse modes are called multi-mode fibers (MMF), while those which can only support a single mode are called single-mode fibers (SMF). Multi-mode fibers generally have a larger 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 550 meters (600 yards).

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 together with an electric arc. Special connectors are used to make removable connections.

Principle of operation

An optical fiber is a cylindrical dielectric 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. 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*.

1)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 actual speed of light in a vacuum is about 300 million meters (186 thousand 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 1.46. The core value is typically 1.48. The larger the index of refraction, the more slowly light travels in that medium.

2)Total internal reflection

When light traveling in a dense medium hits a boundary at a steep angle (larger than the "critical angle" for the boundary), the light will be completely reflected. This effect is used in optical fibers to confine light in the core. Light travels along the fiber bouncing back and forth off of the boundary. 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

Types of Optical fibers:

1)Graded-index fiber

In fiber optics, a graded-index or gradient-index fiber is an optical fiber whose core has a refractive index that decreases with increasing radial distance from the fiber axis (the imaginary central axis running down the length of the fiber).

Because parts of the core closer to the fiber axis have a higher refractive index than the parts near the cladding, light rays follow sinusoidal paths down the fiber. The advantage of the graded-index fiber compared to multimode step-index fiber is the considerable decrease in modal dispersion.

The most common refractive index profile for a graded-index fiber is very nearly parabolic. The parabolic profile results in continual refocusing of the rays in the core, and minimizes modal dispersion.

2)Step-index profile

For an optical fiber, a step-index profile is a refractive index profile characterized by a uniform refractive index within the core and a sharp decrease in refractive index at the core-cladding interface so that the cladding is of a lower refractive index. The step-index profile corresponds to a power-law index profile with the profile parameter approaching infinity. The step-index profile is used in most single-mode fibers and some multimode fibers.

A step-index fiber is characterized by the core and cladding refractive indices n_1 and n_2 and the core and cladding radii a and b. Examples of standard core and cladding diameters 2a/2b are 8/125, 50/125, 62.5/125, 85/125, or 100/140 (units of µm). The fractional refractive-index change . n_1 is typically between 1.44 and 1.46, andis typically between 0.001 and 0.02.

Step-index optical fiber is generally made by doping high-purity fused silica glass (SiO_2) with different concentrations of materials like titanium, germanium, or boron.

Advantages:

1)Speed: Fiber optic networks operate at high speeds - up into the gigabits
2)Bandwidth: large carrying capacity
3)Distance: Signals can be transmitted further without needing to be "refreshed" or strengthened.
4)Resistance: Greater resistance to electromagnetic noise such as radios, motors or other nearby cables.
5)Maintenance: Fiber optic cables costs much less to maintain.