CSE 686 Internet Programming

Week 2: Basic Network Concepts

Edmund Yu, PhD
Associate Teaching Professor
esyu@syr.edu

January 22, 24, 2018

Package java.net

Provides the classes for implementing networking applications.

See: Description

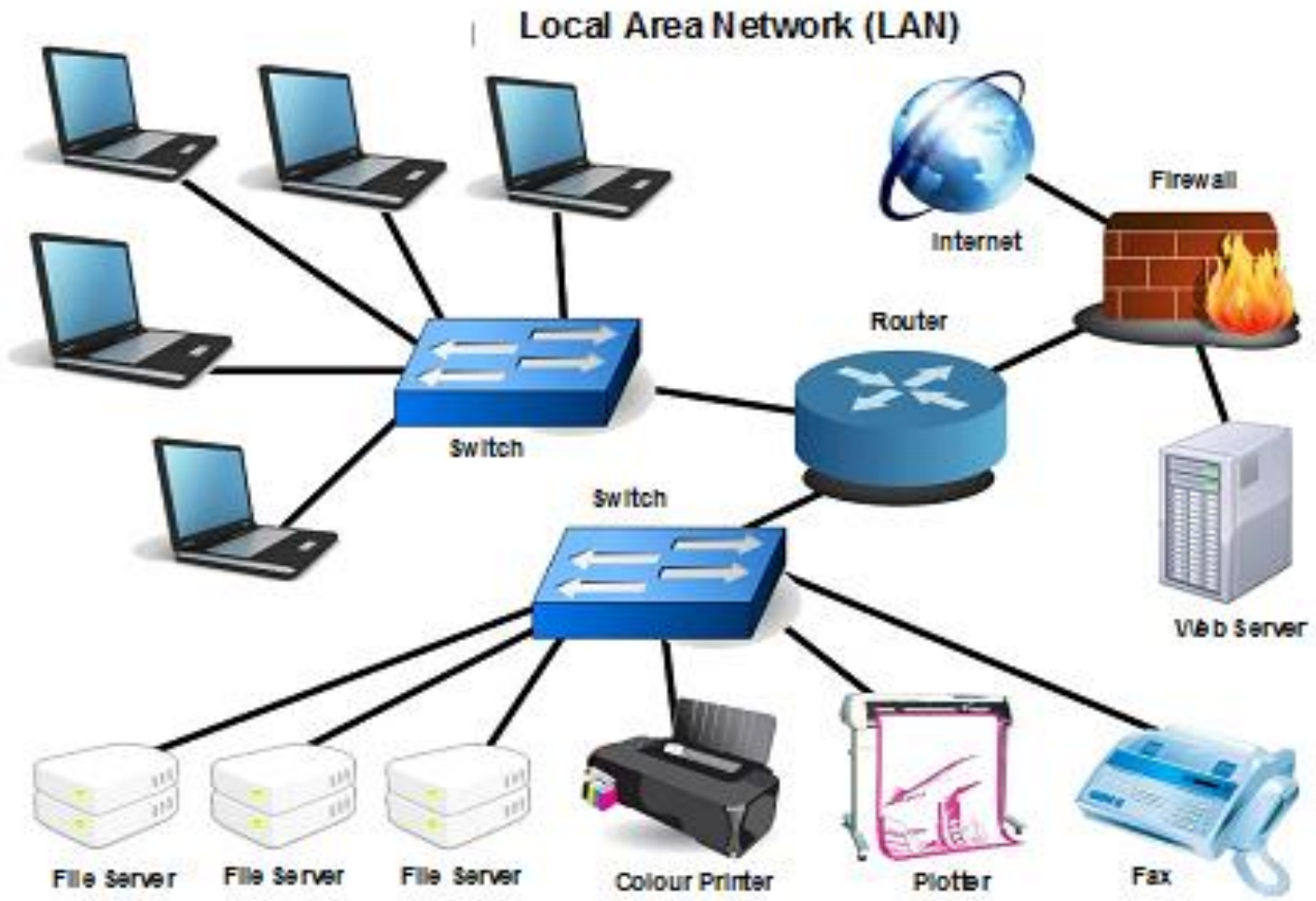
Interface Summary

Interface	Description
ContentHandlerFactory	This interface defines a factory for content handlers.
CookiePolicy	CookiePolicy implementations decide which cookies should be accepted and which should be rejected.
CookieStore	A CookieStore object represents a storage for cookie.
DatagramSocketImplFactory	This interface defines a factory for datagram socket implementations.
FileNameMap	A simple interface which provides a mechanism to map between a file name and a MIME type string.
ProtocolFamily	Represents a family of communication protocols.
SocketImplFactory	This interface defines a factory for socket implementations.
SocketOption<T>	A socket option associated with a socket.

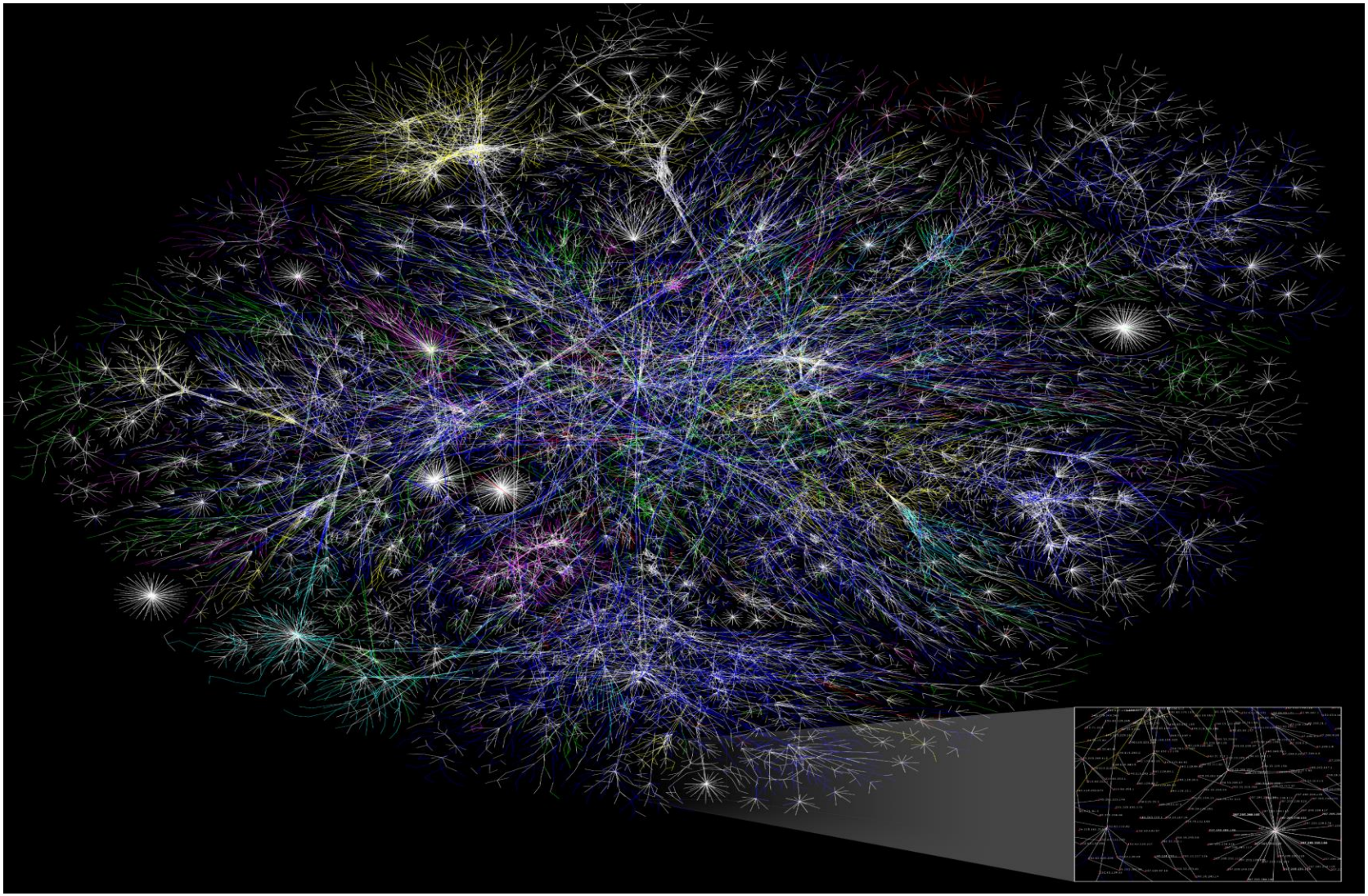
Networks

- A **network**
  - is a collection of computers and other devices that can send data to and receive data from one another, more or less in real time.
  - is often connected by wires, and the bits of data are turned into electromagnetic waves that move through the wires.
    - Wireless networks transmit data using radio waves
    - Most long distance transmissions are now carried over fiber-optic cables that send light waves through glass filaments.
- Theoretically, data could even be transmitted by coal-powered computers that send smoke signals to one another. (From textbook #1)

Networks: LAN



Networks: The Internet



https://en.wikipedia.org/wiki/Internet_Mapping_Project

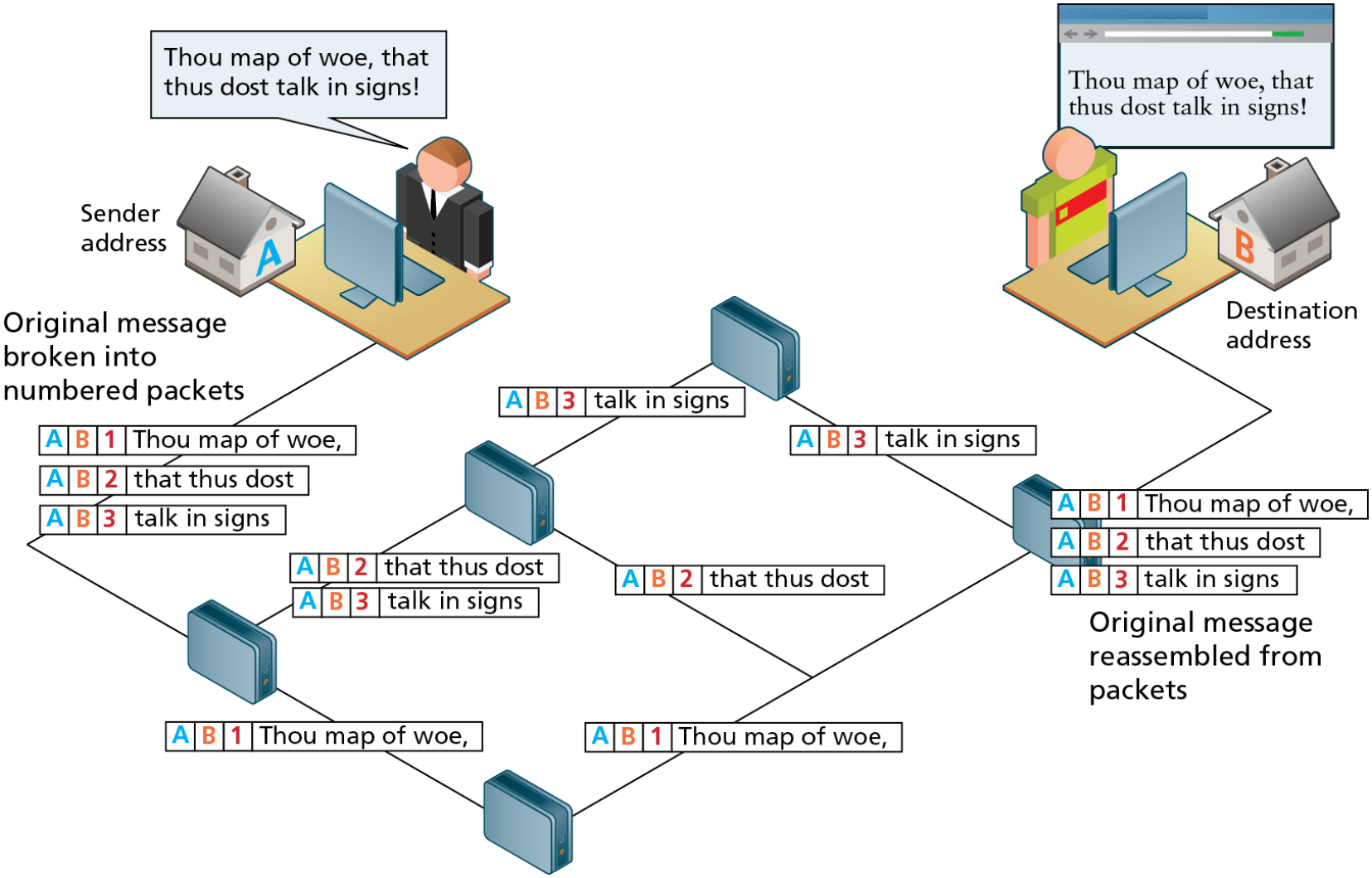
Nodes

- Each machine on a network is called a **node**.
  - Most nodes are computers, but printers, switches, routers, bridges, gateways, dumb terminals, and Coca-Cola machines can also be nodes.
  - You might use Java to interface with a Coke machine, but otherwise you'll mostly talk to other computers.
- Nodes that are fully functional computers are also called **hosts**.

Packets

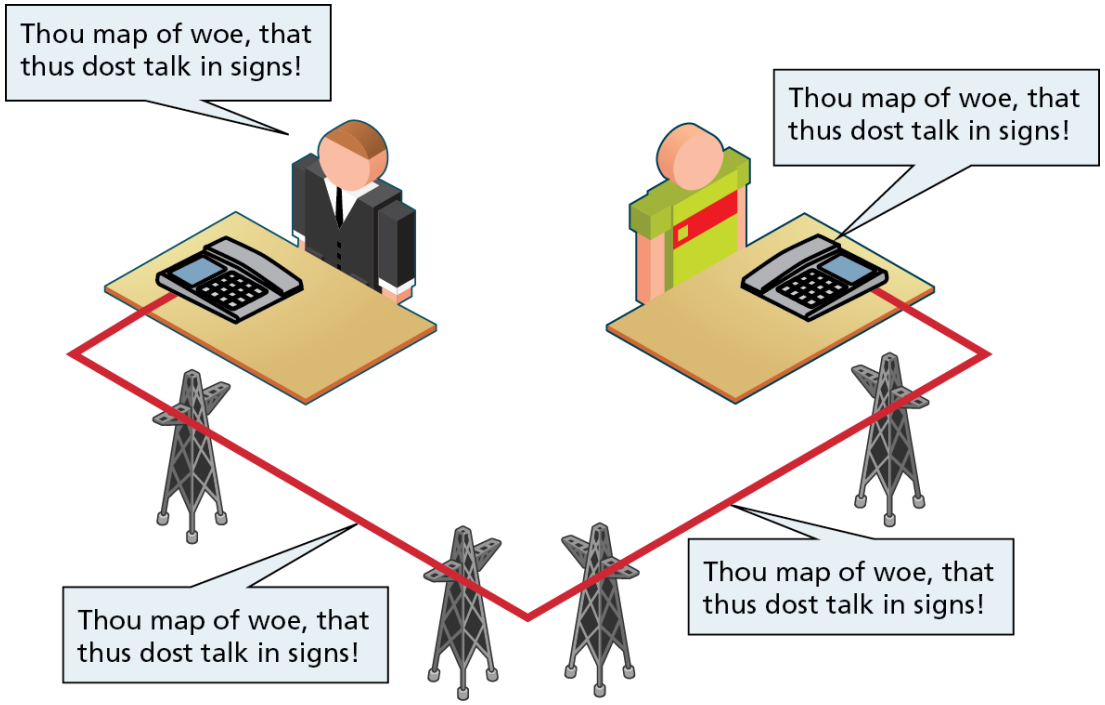
- All modern computer networks are **packet-switched** networks
  - Data traveling on the network is broken into chunks called **packets**.
  - Each packet is handled separately.
  - Each packet contains information about who sent it and where it's going.

Packet Switching (Revisited)



Circuit Switching (Revisited)

- A **circuit switching** establishes an actual physical connection between two people through a series of physical switches.



Circuit Switching (Revisited)

- **Circuit Switching Weaknesses**

1. You must establish a link and maintain a dedicated circuit for the duration of the call
2. Difficult to have multiple conversations simultaneously
3. Wastes bandwidth since even the silences are transmitted

Packet Switching (Revisited)

- While **packet switching** may seem a more complicated and inefficient approach than **circuit switching**, it is:
  - more robust (it is not reliant on a single pathway that may fail)
  - a more efficient use of network resources (since a circuit can communicate multiple connections).

Addresses

- Every network node has an **address**, a sequence of bytes that uniquely identifies it.
  - The more bytes there are in each address, the more devices that can be connected to the network simultaneously.
- Addresses are assigned differently on different kinds of networks:
  - **Ethernet addresses** are attached to the physical Ethernet hardware.
    - Manufacturers of Ethernet hardware use pre-assigned codes. (MAC Address, next slide)
  - **Internet addresses** are normally assigned to a computer by the organization that is responsible for it.
    - However, the addresses that an organization is allowed to choose for its computers are assigned by the organization's ISP.
    - ISPs in turn get their IP addresses from one of four regional Internet registries (e.g. American Registry for Internet Numbers, ARIN).

      → Internet Corporation for Assigned Names and Numbers (ICANN).

MAC address

From Wikipedia, the free encyclopedia

This article is about a type of network address. For the Apple computers, see Macintosh. For other similar terms, see Mac.

A **media access control address** (**MAC address**) of a device is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi-Fi. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.

Label of a UMTS router with MAC addresses for LAN and WLAN modules

MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the **burned-in address** (**BIA**). It may also be known as an **Ethernet hardware address** (**EHA**), **hardware address** or *physical address* (not to be confused with a memory physical address). This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address.

A network node may have multiple NICs and each NIC must have a unique MAC address. Sophisticated network equipment such as a multilayer switch or router may require one or more permanently assigned MAC addresses.

MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): **MAC-48**, **EUI-48**, and **EUI-64**. The IEEE claims trademarks on the names EUI-48[1] and EUI-64,[2] in which EUI is an abbreviation for **Extended Unique Identifier**.

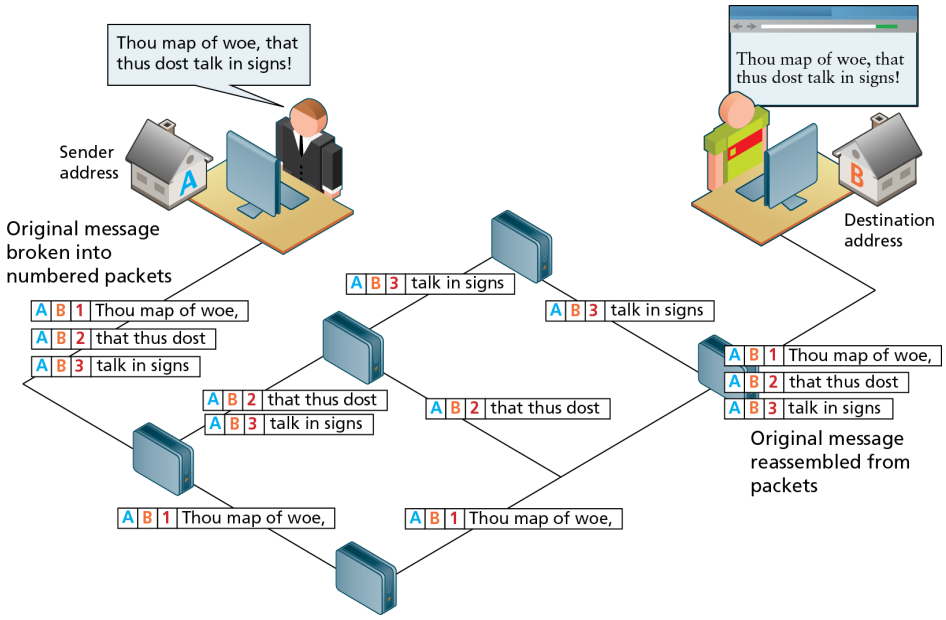
Contents [hide]

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store
Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page
Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page
Print/export

Protocols

- The internet exists today because of a suite of interrelated communications protocols. (TCP/IP)
- A **protocol** is a set of rules that partners in communication use when they communicate.

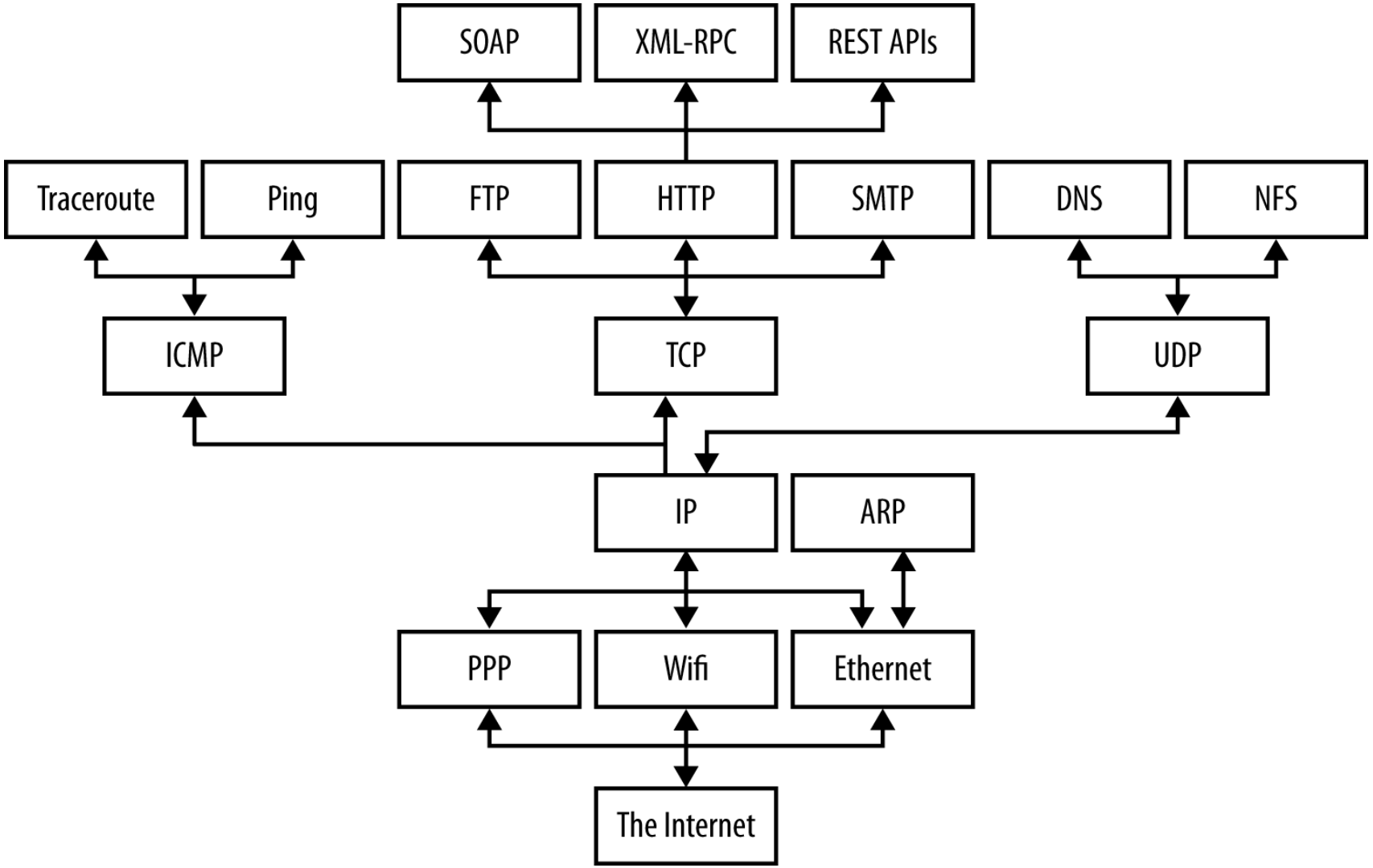
- More precisely, a **protocol** is a clearly-defined set of rules defining how computers communicate, including:
  - the format of addresses
  - how data is split into packets



Protocols

- There are many different protocols defining different aspects of network communication. (See next slide)
  - E.g. the Hypertext Transfer Protocol (HTTP) defines how web browsers and servers communicate
- Open, published protocol standards allow software and equipment from different vendors to communicate with one another.
  - A web server doesn't care whether the client is a Unix workstation, an Android phone, or an iPad, because all clients speak the same HTTP protocol regardless of platform.

Protocols


SOAP
XML-RPC
REST APIs
Traceroute
Ping
FTP
HTTP
SMTP
DNS
NFS
ICMP
TCP
UDP
IP
ARP
PPP
Wifi
Ethernet
The Internet

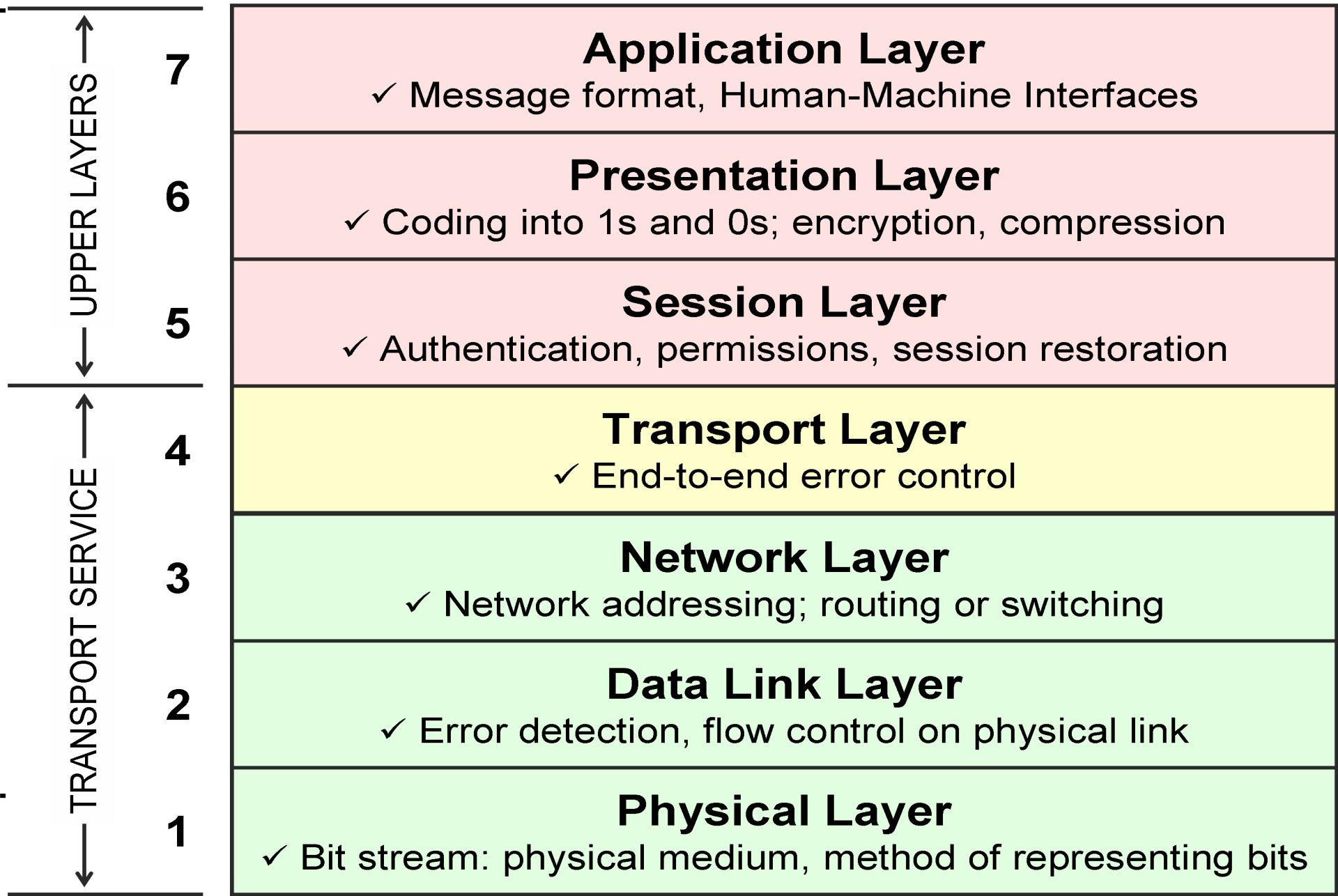
The Layers of a Network

- To hide most of this complexity from the application developer and end user, different aspects of network communication are separated into multiple layers.
  - Each layer represents a different level of abstraction between the physical hardware (i.e., the wires and electricity) and the information being transmitted.
  - In theory, each layer only talks to the layers immediately above and immediately below it.
  - Separating the network into layers lets you modify or even replace the software in one layer without affecting the others, as long as the interfaces between the layers stay the same.

The Layered Architecture Pattern

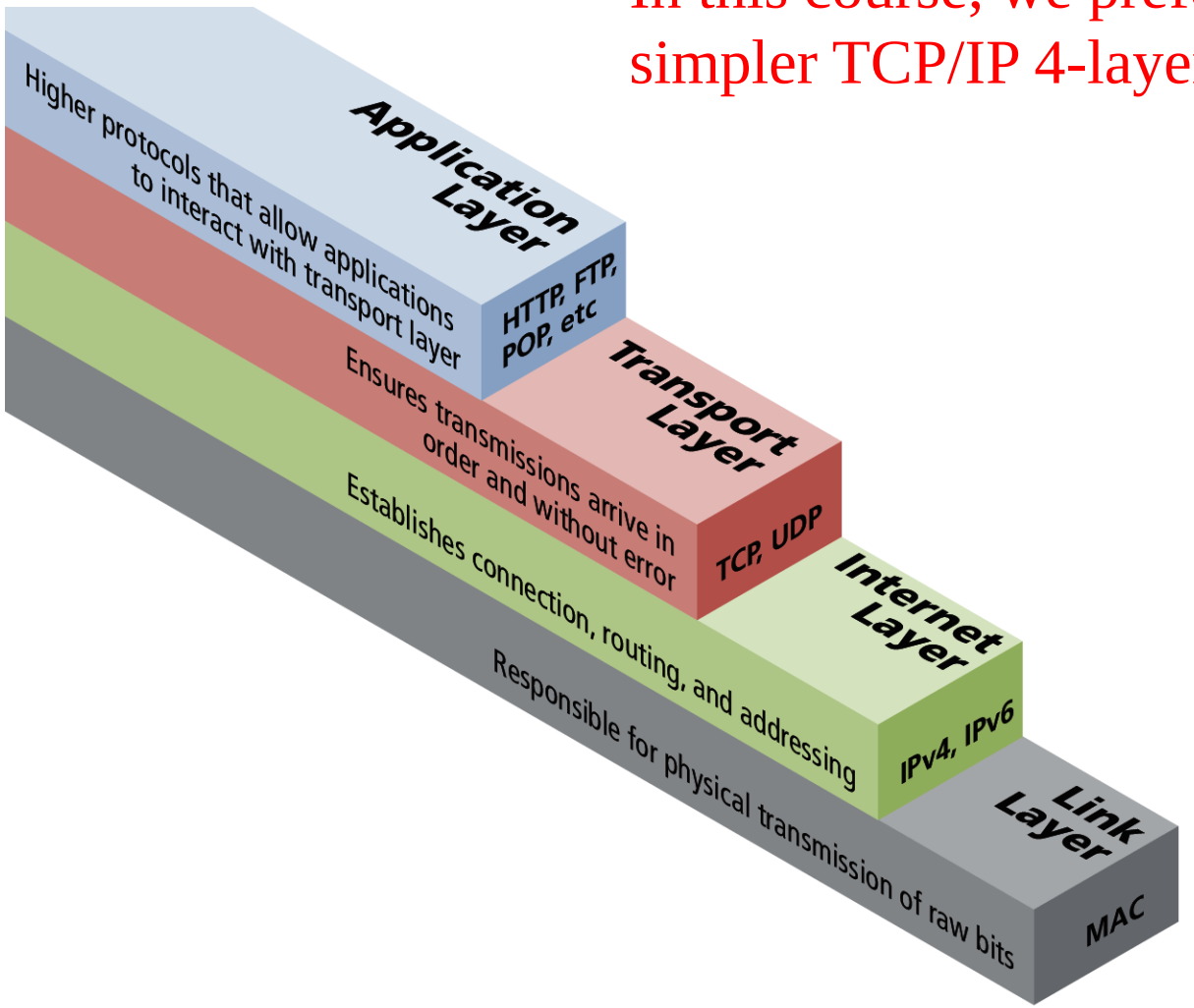
Name	Layered architecture
Description	Organizes the system into layers, with related functionality associated with each layer. A layer provides services to the layer above it, so the lowest level layers represent core services that are likely to be used throughout the system. See Figure 6.8.
Example	A layered model of a digital learning system to support learning of all subjects in schools (Figure 6.9).
When used	Used when building new facilities on top of existing systems; when the development is spread across several teams with each team responsibility for a layer of functionality; when there is a requirement for multilevel security.
Advantages	Allows replacement of entire layers as long as the interface is maintained. Redundant facilities (e.g., authentication) can be provided in each layer to increase the dependability of the system.
Disadvantages	In practice, providing a clean separation between layers is often difficult, and a high-level layer may have to interact directly with lower-level layers rather than through the layer immediately below it. Performance can be a problem because of multiple levels of interpretation of a service request as it is processed at each layer.

OSI (Open Systems Interconnection) 7-Layer Model

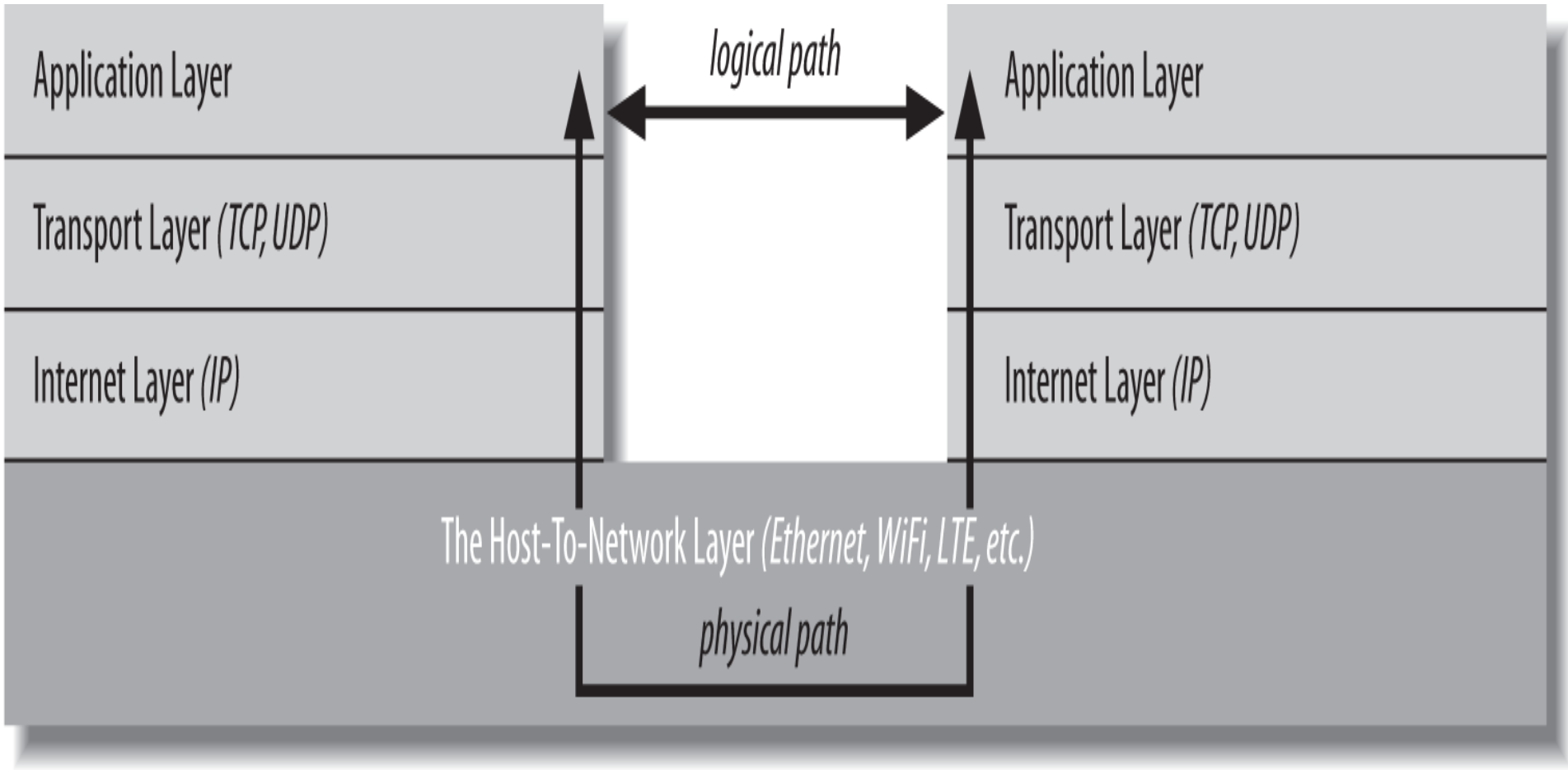


The TCP/IP 4-Layer Model

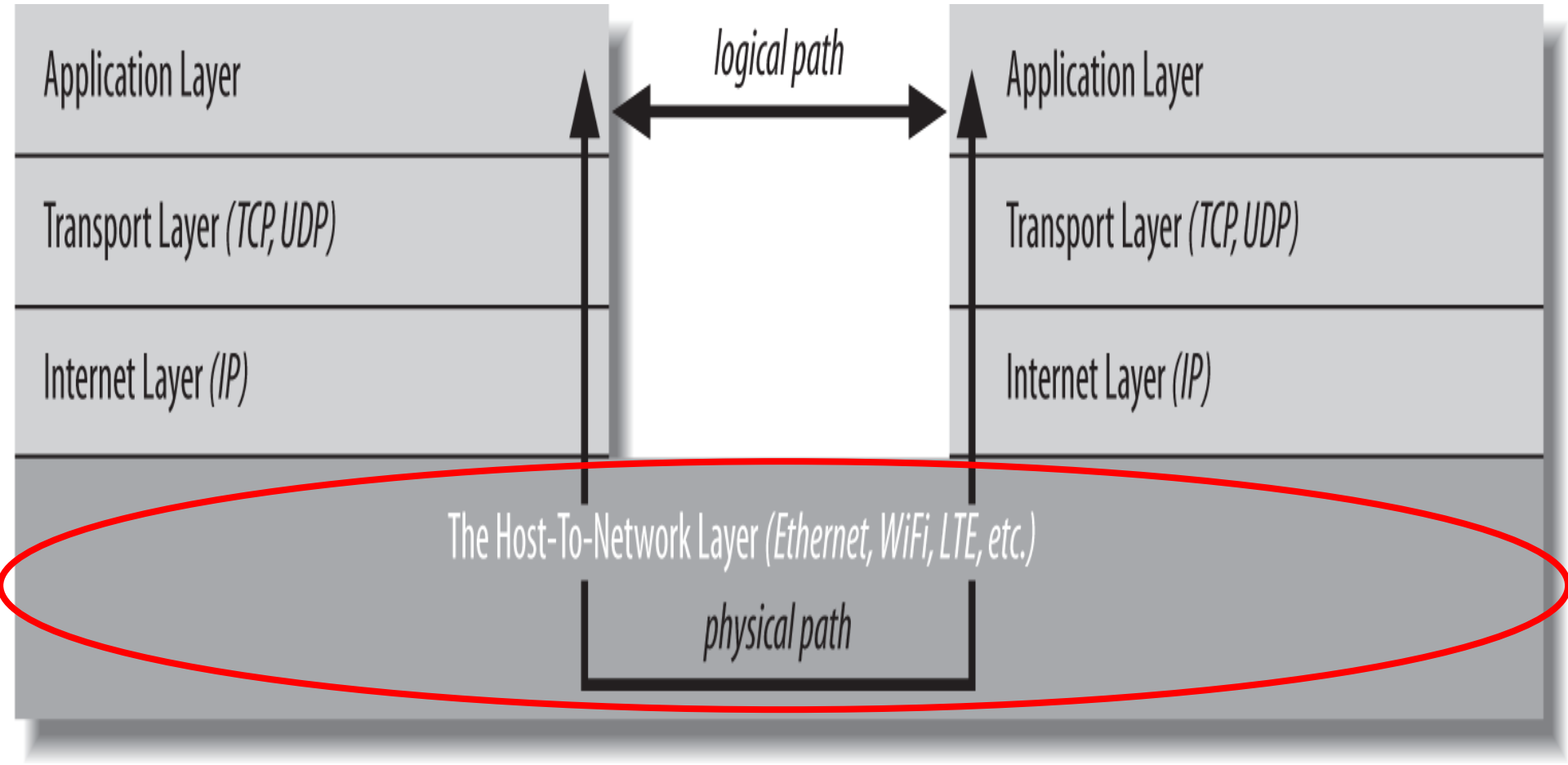
In this course, we prefer to use this simpler TCP/IP 4-layer model.



The TCP/IP 4-Layer Model



The TCP/IP 4-Layer Model



WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link

LTE (telecommunication)

From Wikipedia, the free encyclopedia

> *"Long-term evolution" redirects here. For the biological concept, see Evolution and E. coli long-term evolution experiment.*

In telecommunication, **Long-Term Evolution** (**LTE**) is a standard for high-speed wireless communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies. It increases the capacity and speed using a different radio interface together with core network improvements.[1][2] The standard is developed by the 3GPP (3rd Generation Partnership Project) and is specified in its Release 8 document series, with minor enhancements described in Release 9. LTE is the upgrade path for carriers with both GSM/UMTS networks and CDMA2000 networks. The different LTE frequencies and bands used in different countries mean that only multi-band phones are able to use LTE in all countries where it is supported.

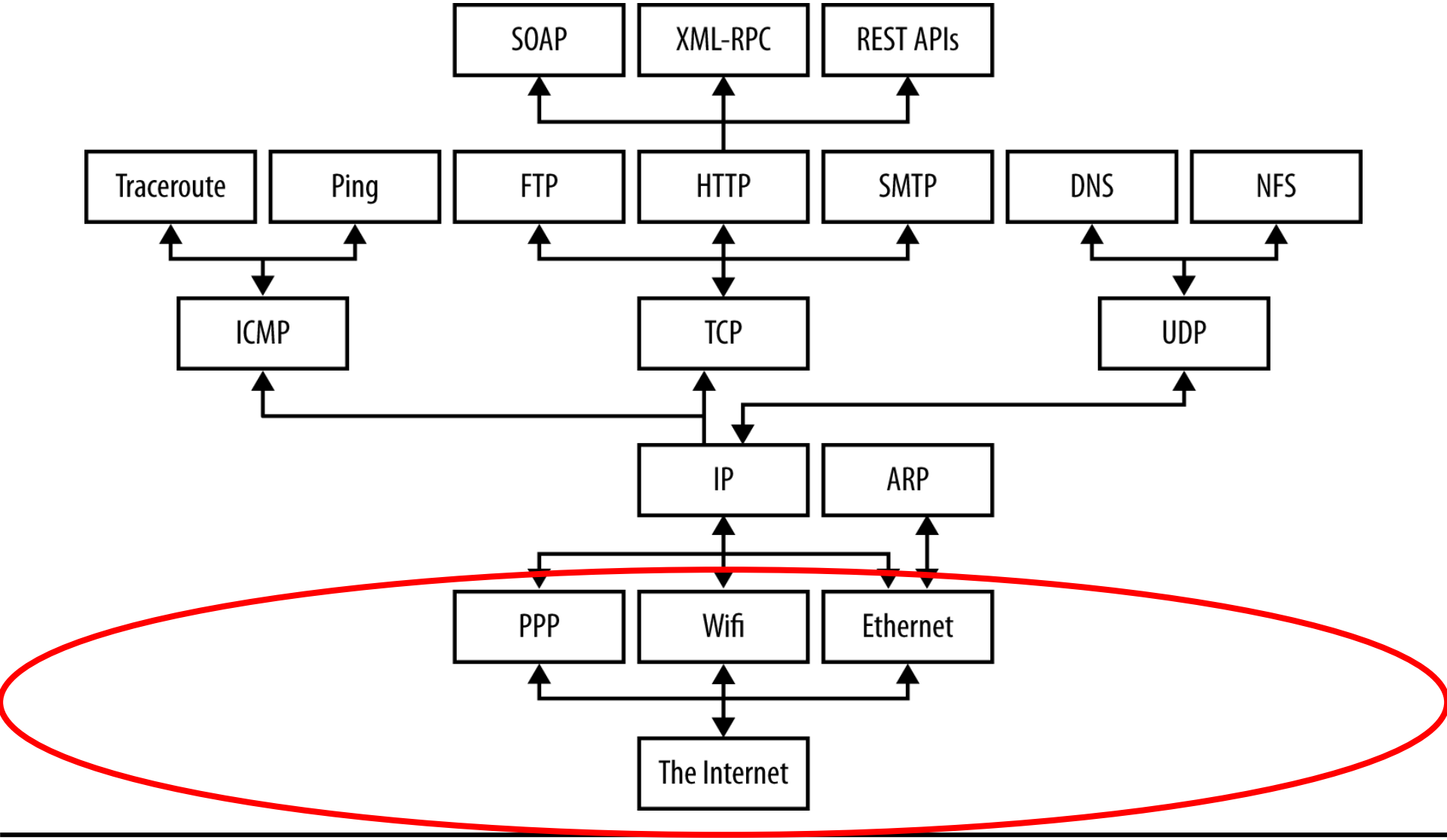
LTE is commonly marketed as **4G LTE**, but it does not meet the technical criteria of a 4G wireless service, as specified in the 3GPP Release 8 and 9 document series, for LTE Advanced. The requirements were originally set forth by the ITU-R organization in the IMT Advanced specification. However, due to marketing pressures and the significant advancements that WiMAX, Evolved High Speed Packet Access and LTE bring to the original 3G technologies, ITU later decided that LTE together with the aforementioned technologies can be called 4G technologies.[3] The LTE Advanced standard formally satisfies the ITU-R requirements to be considered IMT-Advanced.[4] To differentiate LTE Advanced and WiMAX-Advanced from current 4G technologies, ITU has defined them as "True 4G".[5][6]

Contents [hide]

The Host-to-Network Layer

- In the standard model for IP-based Internets, the hidden parts of the network belong to the **host-to-network layer** (also known as the link layer, data link layer, or network interface layer).
- The host-to-network layer defines how a particular network interface, such as an Ethernet card or a WiFi antenna, sends IP packets over its physical connection to the local network and the world.
- The primary reason you'll need to think about this layer is performance:
  - reliable fiber-optic connections vs Ethernet connections
  - 4G satellite connections vs WiFi, etc.

Protocols


SOAP
XML-RPC
REST APIs
Traceroute
Ping
FTP
HTTP
SMTP
DNS
NFS
ICMP
TCP
UDP
IP
ARP
PPP
Wifi
Ethernet
The Internet

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link

Point-to-Point Protocol

From Wikipedia, the free encyclopedia

This article includes a list of references, but **its sources remain unclear** because it has **insufficient inline citations**. Please help to improve this article by introducing more precise citations. *(November 2011) (Learn how and when to remove this template message)*

In computer networking, **Point-to-Point Protocol** (**PPP**) is a data link layer (layer 2) communications protocol used to establish a direct connection between two nodes. It connects two routers directly without any host or any other networking device in between. It can provide connection authentication, transmission encryption,[1] and compression.

PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as SONET. Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet, since IP packets cannot be transmitted over a modem line on their own, without some data link protocol.

Two derivatives of PPP, Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over ATM (PPPoA), are used most commonly by

Internet protocol suite

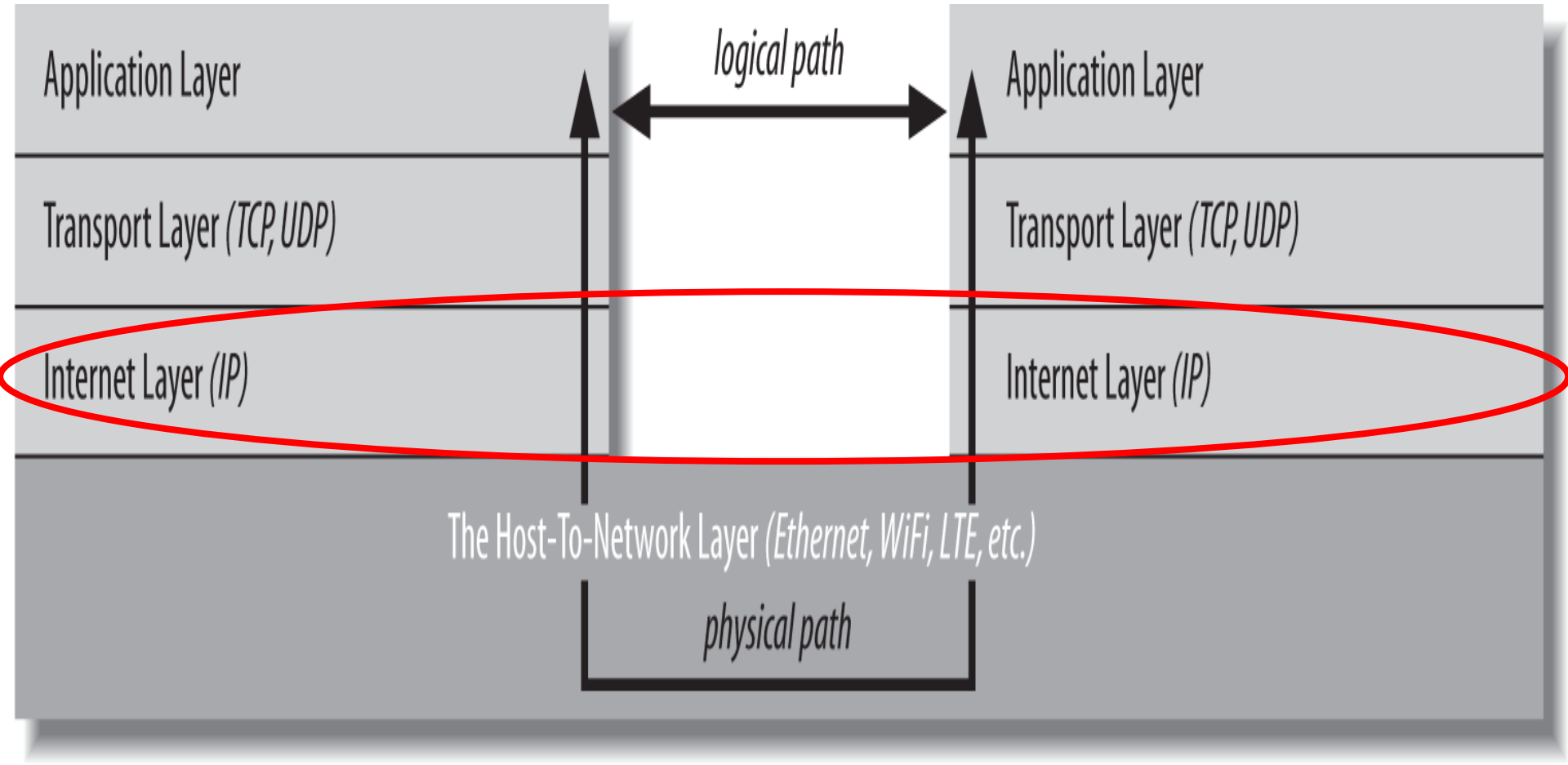
Application layer
BGP · DHCP · DNS · FTP · HTTP · IMAP · LDAP · MGCP · MQTT · NNTP · NTP · POP · ONC/RPC · RTP · RTSP · RIP · SIP · SMTP · SNMP · SSH · Telnet · TLS/SSL · XMPP · *more...*

Transport layer
TCP · UDP · DCCP · SCTP · RSVP · *more...*

Internet layer
IP (IPv4 · IPv6) · ICMP · ICMPv6 · ECN · IGMP · IPsec · OSPF · *more...*

Link layer
ARP · NDP · Tunnels (L2TP) · **PPP** · MAC (Ethernet · DSL · ISDN · FDDI) · *more...*

The TCP/IP 4-Layer Model

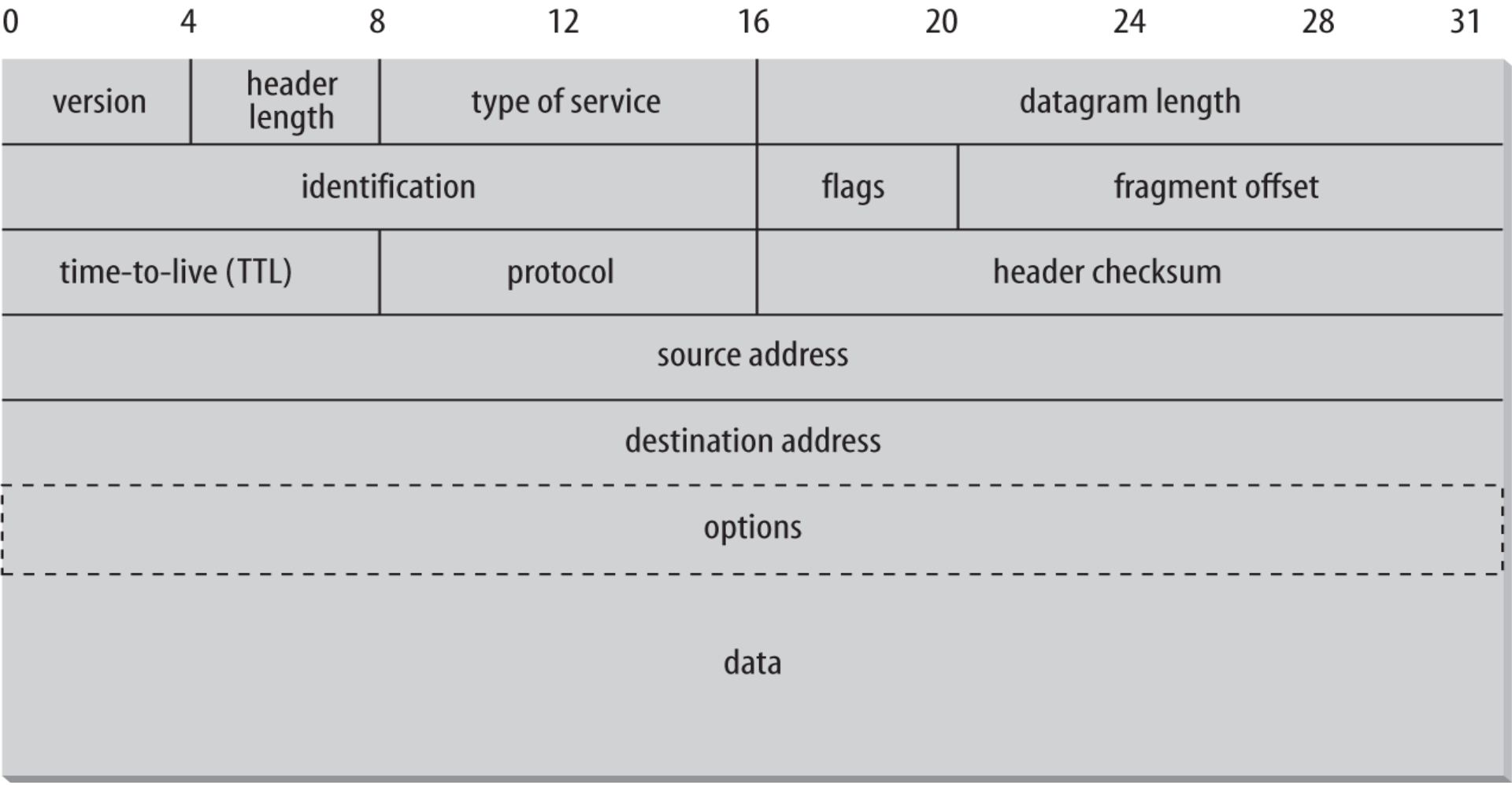


The Internet Layer

- In the OSI model, the internet layer goes by the more generic name network layer.
- A network layer protocol defines
  - how bits and bytes of data are organized into the larger groups called packets (See next slide)
  - the addressing scheme by which different machines find one another.
- The Internet Protocol (IP):
  - The most widely used network layer protocol in the world
  - The only network layer protocol Java understands.
  - Has 2 versions:
    - IPv4 - uses **32**-bit addresses
    - IPv6 - uses **128**-bit addresses and adds a few other technical features to assist with routing.

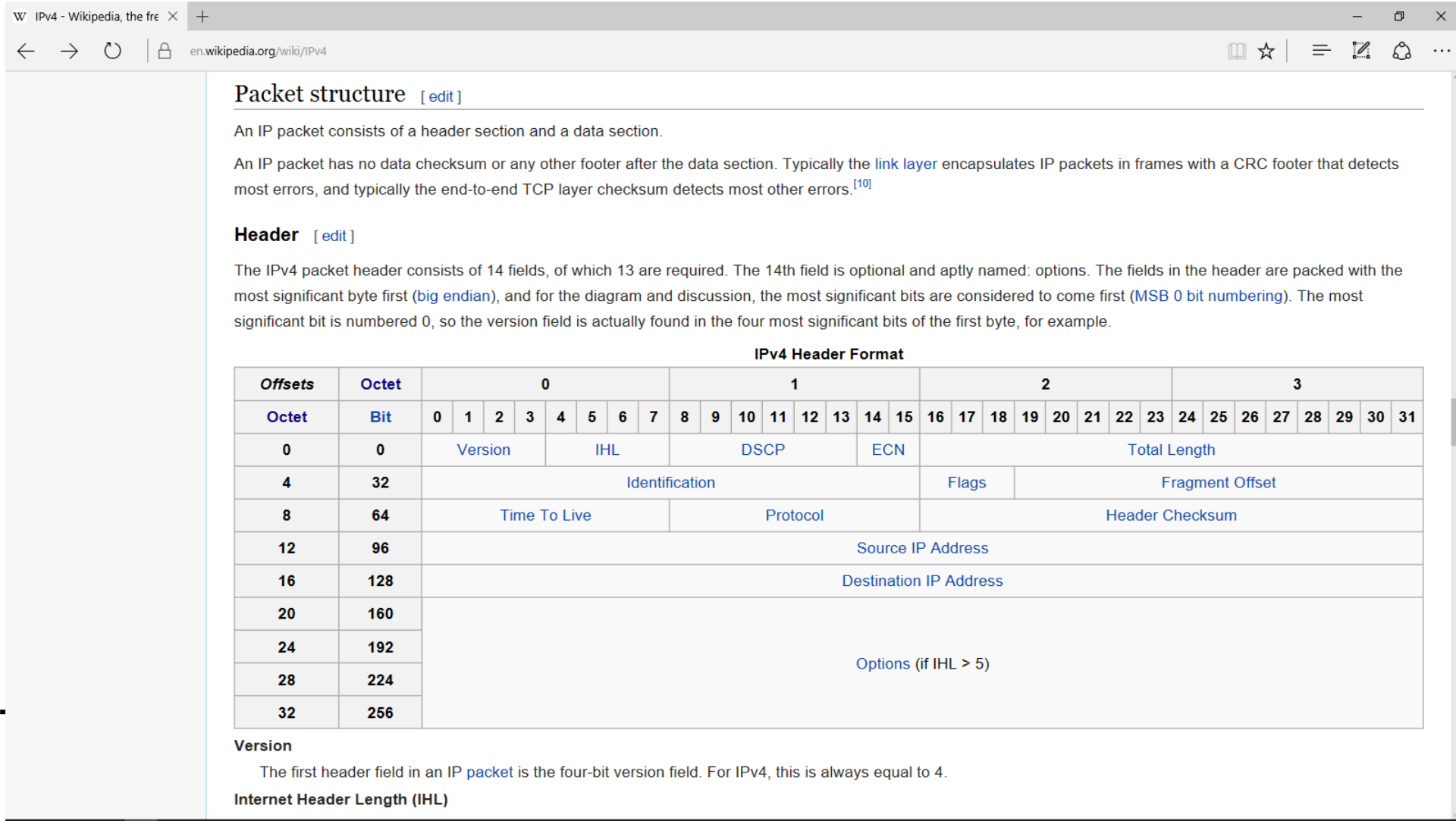
Datagrams

- In both IPv4 and IPv6, data is sent across the internet layer in packets called **datagrams**:



Datagrams

- In both IPv4 and IPv6, data is sent across the internet layer in packets called **datagrams**:



Packet structure [edit]

An IP packet consists of a header section and a data section.

An IP packet has no data checksum or any other footer after the data section. Typically the link layer encapsulates IP packets in frames with a CRC footer that detects most errors, and typically the end-to-end TCP layer checksum detects most other errors.[10]

Header [edit]

The IPv4 packet header consists of 14 fields, of which 13 are required. The 14th field is optional 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	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags				Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
24	192																																
28	224																																
32	256																																

Version

The first header field in an IP packet is the four-bit version field. For IPv4, this is always equal to 4.

Internet Header Length (IHL)

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

In other projects
Wikimedia Commons

Languages
العربية
Azərbaycanca

IPv6

From Wikipedia, the free encyclopedia

Internet Protocol version 6 (**IPv6**) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.[1]

Every device on the Internet is assigned an IP address for identification and location definition. With the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses than the IPv4 address space has available were necessary to connect new devices in the future. By 1998, the Internet Engineering Task Force (IETF) had formalized the successor protocol. IPv6 uses a 128-bit address, theoretically allowing 2^{128}, or approximately 3.4×10^{38} addresses. The actual number is slightly smaller, as multiple ranges are reserved for special use or completely excluded from use. The total number of possible IPv6 addresses is more than 7.9×10^{28} times as many as IPv4, which uses 32-bit addresses and provides approximately 4.3 billion addresses. The two protocols are not designed to be interoperable, complicating the transition to IPv6. However, several IPv6 transition mechanisms have been devised to permit communication between IPv4 and IPv6 hosts.

Internet protocol suite

Application layer
BGP · DHCP · DNS · FTP · HTTP · IMAP · LDAP · MGCP · NNTP · NTP · POP · ONC/RPC · RTP · RTSP · RIP · SIP · SMTP · SNMP · SSH · Telnet · TLS/SSL · XMPP · *more...*

Transport layer
TCP · UDP · DCCP · SCTP · RSVP · *more...*

Internet layer
IP (IPv4 · **IPv6**) · ICMP · ICMPv6 · ECN · IGMP · IPsec · *more...*

Link layer
ARP · NDP · OSPF · Tunnels (L2TP) · PPP · MAC (Ethernet · DSL · ISDN · FDDI) · *more...*

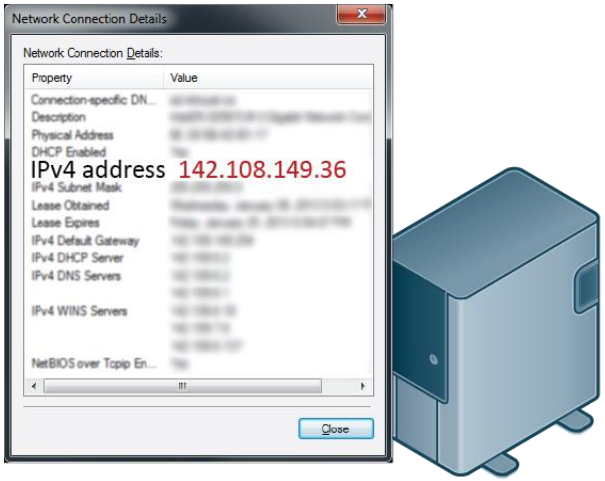
V · T · E

IPv6 provides other technical benefits in addition to a larger addressing space. In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables. The use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services. Device mobility, security, and configuration aspects have been considered in the design of the protocol.

IPv6 addresses are represented as eight groups of four hexadecimal digits with the groups being separated by colons, for example 2001:0db8:0000:0042:0000:8a2e:0370:7334, but methods to abbreviate this full notation exist.

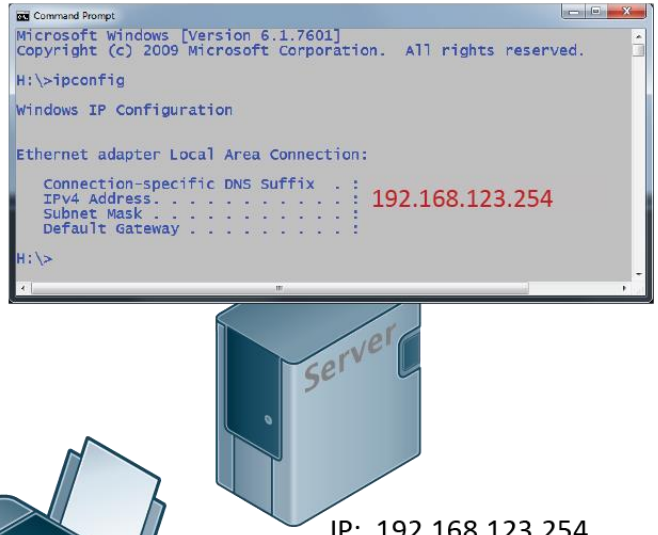
Contents [hide]

IP Addresses

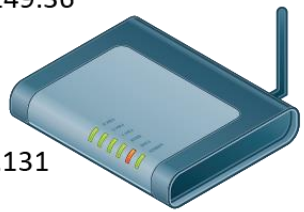


IP: 142.108.149.36

IP: 22.15.216.13

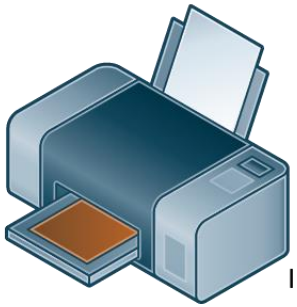


IP: 192.168.123.254



IP: 10.238.28.131

IP: 10.239.28.131

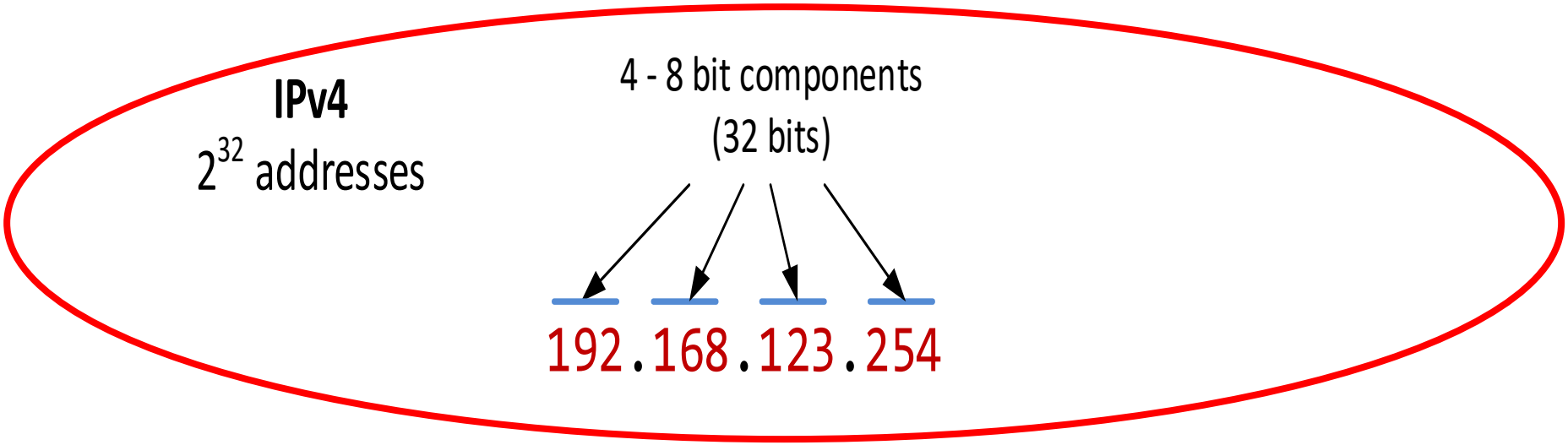


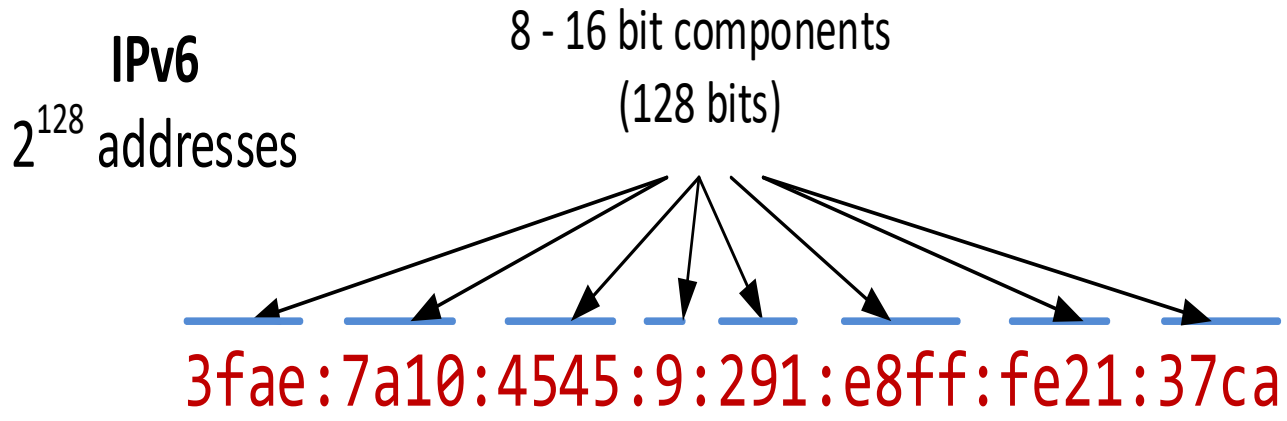
IP: 142.181.80.3

IP Addresses

- **IPv4** addresses are the IP addresses from the original TCP/IP protocol. Every computer on an IPv4 network is identified by a four-byte number
  - **dotted quad** → 128.230.171.184
  - Each of the four numbers is one unsigned byte ranging in value from 0 to 255.
- When data is transmitted across the network, the packet's header includes:
  - the destination address - the address of the machine for which the packet is intended
  - the source address - the address of the machine that sent the packet, included so the recipient knows whom to reply to
- Routers along the way choose the best route on which to send the packet by inspecting the destination address.

IPv4 vs IPv6


IPv4
2^{32} addresses
4 - 8 bit components
(32 bits)
192.168.123.254


IPv6
2^{128} addresses
8 - 16 bit components
(128 bits)
3fae:7a10:4545:9:291:e8ff:fe21:37ca

IP Addresses

- Since an unsigned 8-bit integer's maximum value is 255, four integers together can encode approximately 4.2 billion unique IP addresses.
  - In April 2011, Asia and Australia ran out.
    - No more IPv4 addresses were available to be allocated to these regions
  - In September 2012, Europe ran out too.
  - In September 2015, North America ran out too.
  - Latin America, and Africa only have a few IP addresses left
- A slow transition is under way to **IPv6**, which will use 16-byte addresses.

IP Addresses

http://www.networkworld.com/article/2985340/ipv6/arin-finally-run

ARIN Finally Runs Out of IP...

NETWORKWORLD FROM IDG

INSIDER Sign In | Register

CORE NETWORKING AND SECURITY

By Scott Hogg | Follow

About

Scott Hogg is the CTO for Global Technology Resources, Inc. (GTRI). Scott provides network engineering, security consulting, and training services to his clients.

MORE

OPINION

ARIN Finally Runs Out of IPv4 Addresses

IPv4 Address Cupboards are Bare in North America.

Network World | Sep 22, 2015 7:25 AM PT

RELATED

An insider's guide to the private IPv4 market

Techniques for Prolonging the Lifespan of IPv4

ARIN's registry and transfer policies can help bridge the gap from IPv4 to IPv6

on IDG Answers

If I buy a Chromebook and can't get to grips with OS can I convert to windows?

Find and fix problems fast to deliver exceptional user experiences

IP Addresses

- IPv6 addresses are customarily written in eight blocks of four hexadecimal digits separated by colons:

  FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

- Leading zeroes do not need to be written.
  - A double colon indicates multiple **zero blocks**.

    *FEDC:**0000:0000:0000**:00DC:**0000**:7076:**00**10* →
    *FEDC::DC:**0**:7076:10*

- In mixed networks of IPv6 and IPv4, the last four bytes of the IPv6 address are sometimes written as an IPv4 dotted quad address.

  *FEDC:BA98:7654:3210:FEDC:BA98:**7654:3210*** →
  *FEDC:BA98:7654:3210:FEDC:BA98:**118.84.50.16***

Special IP Addresses

- Several address blocks and patterns are special:
  - Non-routable addresses
  - Local loopback addresses
  - Broadcast addresses

Non-Routable Addresses

- The following IPv4 addresses are unassigned
  - Addresses that begin with 10.
  - Addresses between 172.16. and 172.31.
  - Addresses that begin with 192.168.
- No host using addresses in these blocks is allowed onto the global Internet.
- These **non-routable** addresses are useful for building **private networks** that can’t be seen on the Internet.

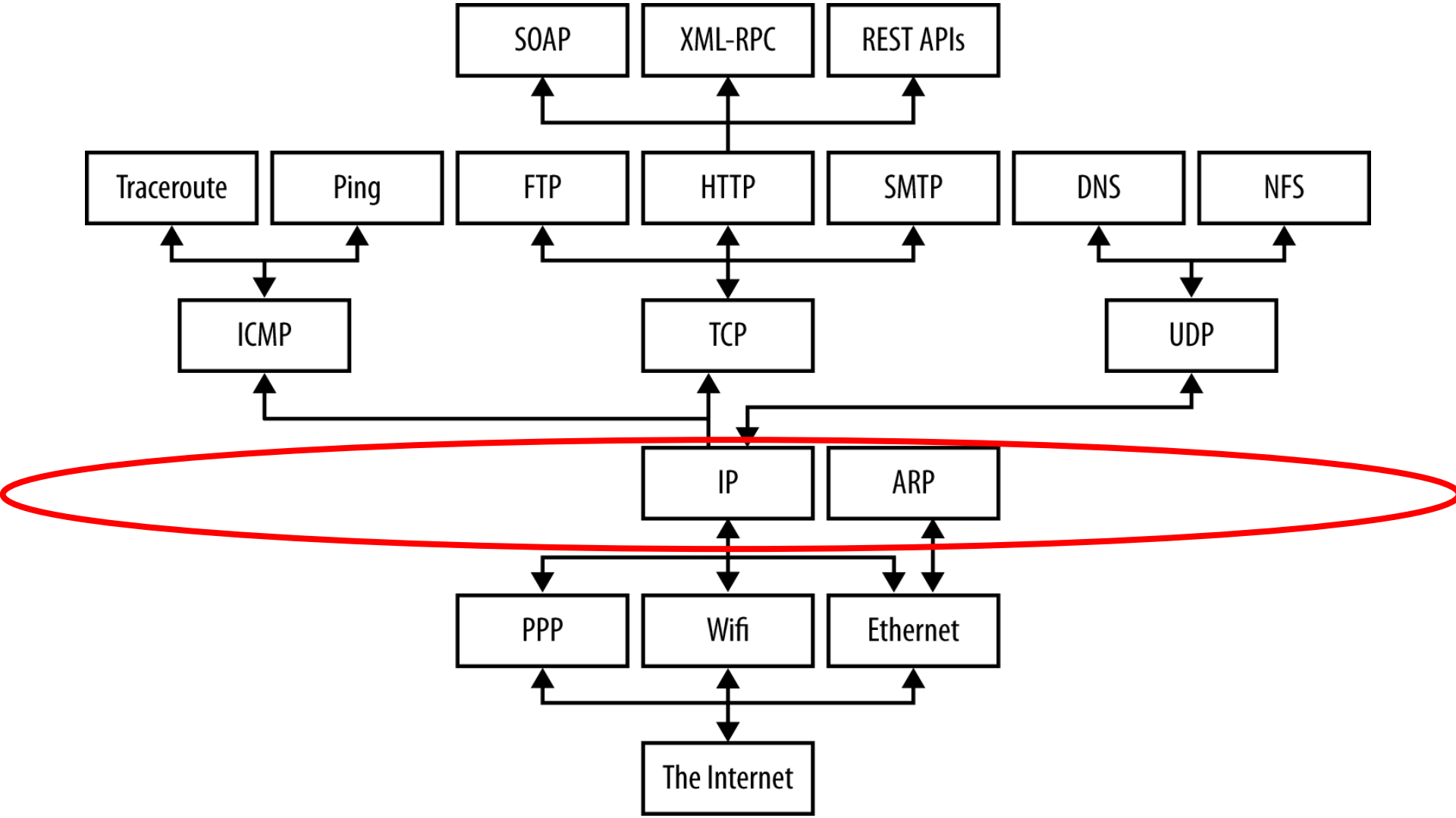
Local Loopback Addresses

- IPv4 addresses beginning with 127 (most commonly **127.0.0.1**) always mean the **local loopback address**.
  - They always point to the local computer, no matter which computer you're running on.
  - The hostname for this address is often **localhost**.
  - In IPv6, 0:0:0:0:0:0:0:1 (a.k.a. ::1) is the loopback address.
- The address **0.0.0.0** always refers to the originating host
  - It may only be used as a source address, not a destination.
- Any IPv4 address that begins with **0.** is assumed to refer to a host on the same local network.

Broadcast Addresses

- The IPv4 address that uses the same number for each of the four bytes (i.e., 255.255.255.255), is a **broadcast address**.
  - Packets sent to this address are received by all nodes on the local network. (For discovery).
- When a client such as a laptop boots up, it sends a particular message to 255.255.255.255 to find the local **Dynamic Host Configuration Protocol (DHCP) server**.
  - All nodes on the network receive the packet, but only the DHCP server responds.
  - The DHCP server sends the laptop information about the local network configuration, including
    - the IP address that laptop should use (just for this session)
    - the address of a DNS server it can use to resolve hostnames.

Protocols


SOAP
XML-RPC
REST APIs
Traceroute
Ping
FTP
HTTP
SMTP
DNS
NFS
ICMP
TCP
UDP
IP
ARP
PPP
Wifi
Ethernet
The Internet

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here

Address Resolution Protocol

From Wikipedia, the free encyclopedia

The **Address Resolution Protocol** (**ARP**) is a communication protocol used for discovering the link layer address associated with a given IPv4 address, a critical function in Internet Protocol (IP) computer networks. ARP was defined in 1982 by RFC 826,[1] which is Internet Standard STD 37.

ARP is used for mapping a network address such as an IPv4 address, to a physical address, such as a MAC address. ARP has been implemented with many combinations of network and data link layer technologies, such as IPv4, Chaosnet, DECnet and Xerox PARC Universal Packet (PUP) using IEEE 802 standards, FDDI, X.25, Frame Relay and Asynchronous Transfer Mode (ATM). IPv4 over IEEE 802.3 and IEEE 802.11 is the most common usage.

In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery Protocol (NDP).

Contents [hide]

Internet protocol suite

Application layer
BGP · DHCP · DNS · FTP · HTTP · IMAP · LDAP · MGCP · MQTT · NNTP · NTP · POP · ONC/RPC · RTP · RTSP · RIP · SIP · SMTP · SNMP · SSH · Telnet · TLS/SSL · XMPP · *more...*

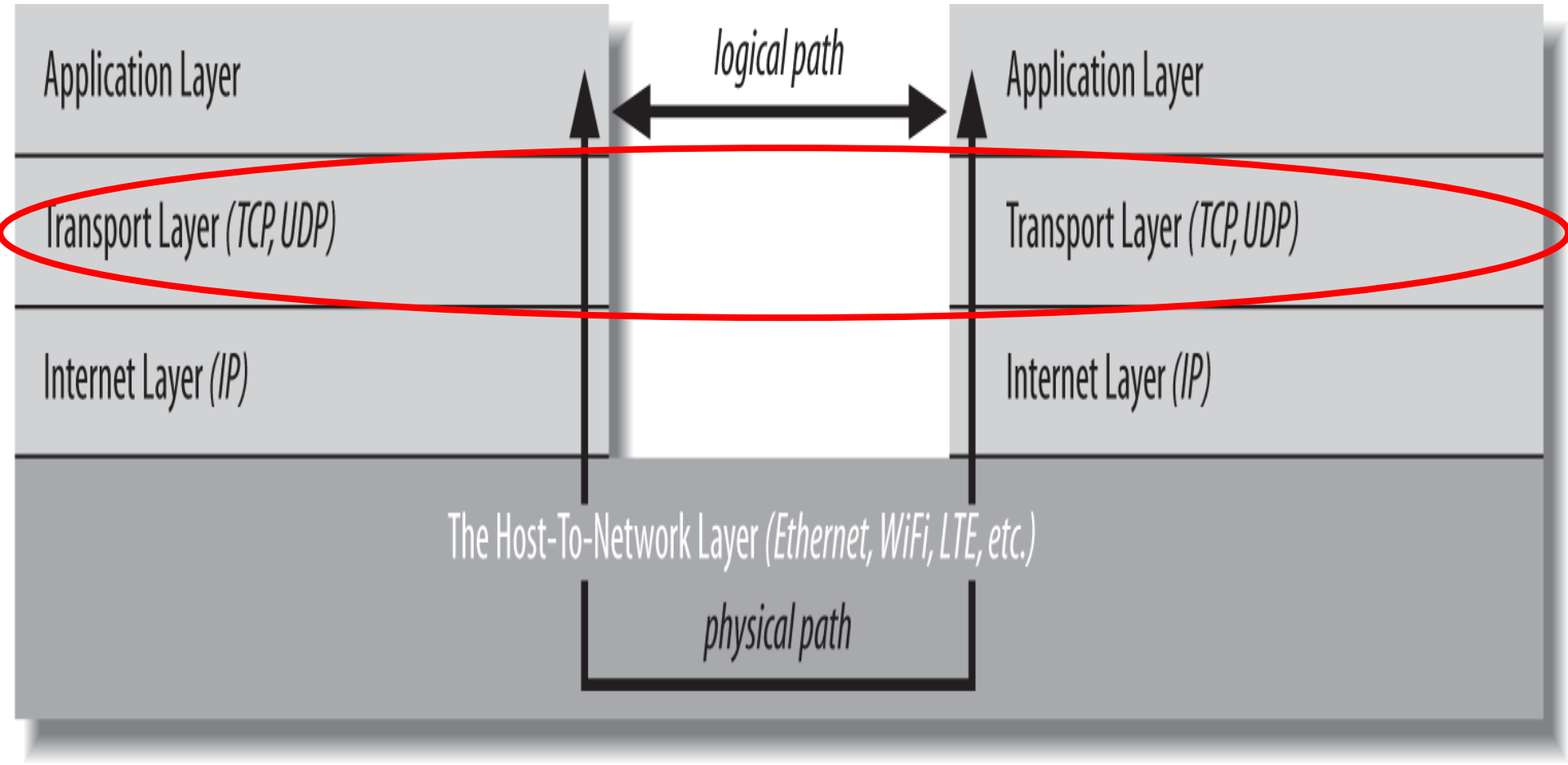
Transport layer
TCP · UDP · DCCP · SCTP · RSVP · *more...*

Internet layer
IP (IPv4 · IPv6) · ICMP · ICMPv6 · ECN · IGMP · IPsec · OSPF · *more...*

Link layer
ARP · NDP · Tunnels (L2TP) · PPP · MAC (Ethernet · DSL · ISDN · FDDI) · *more...*

V · T · E

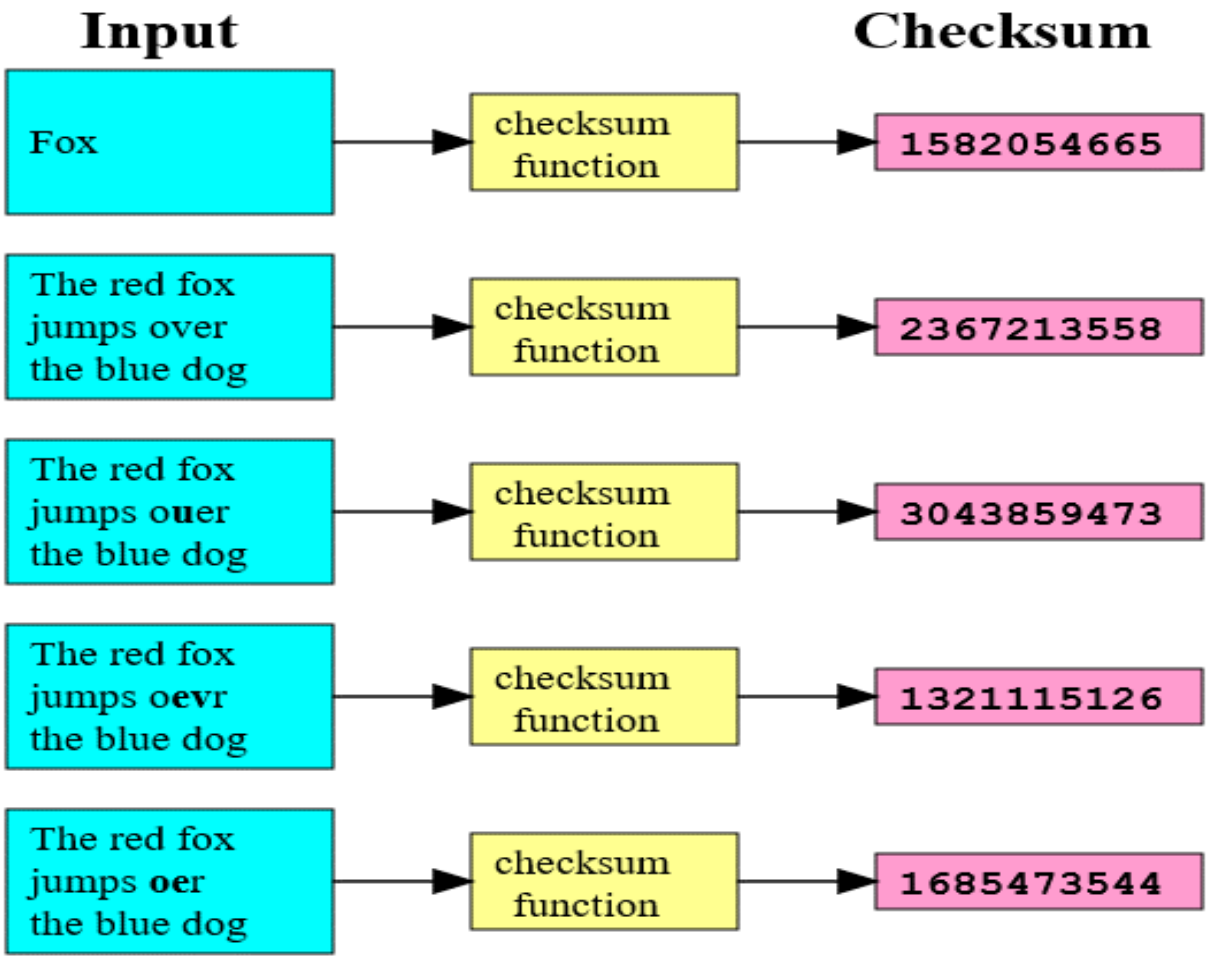
The TCP/IP 4-Layer Model



The Transport Layer

- Raw datagrams have drawbacks:
  - There's no guarantee that they will be delivered.
  - Even if they are delivered, they may have been corrupted in transit.
    - The header **checksum** can only detect corruption in the header, not in the data portion of a datagram.
  - Even if the datagrams arrive uncorrupted, they do not necessarily arrive in the order in which they were sent.
    - Individual datagrams may follow different routes from source to destination.

Checksum



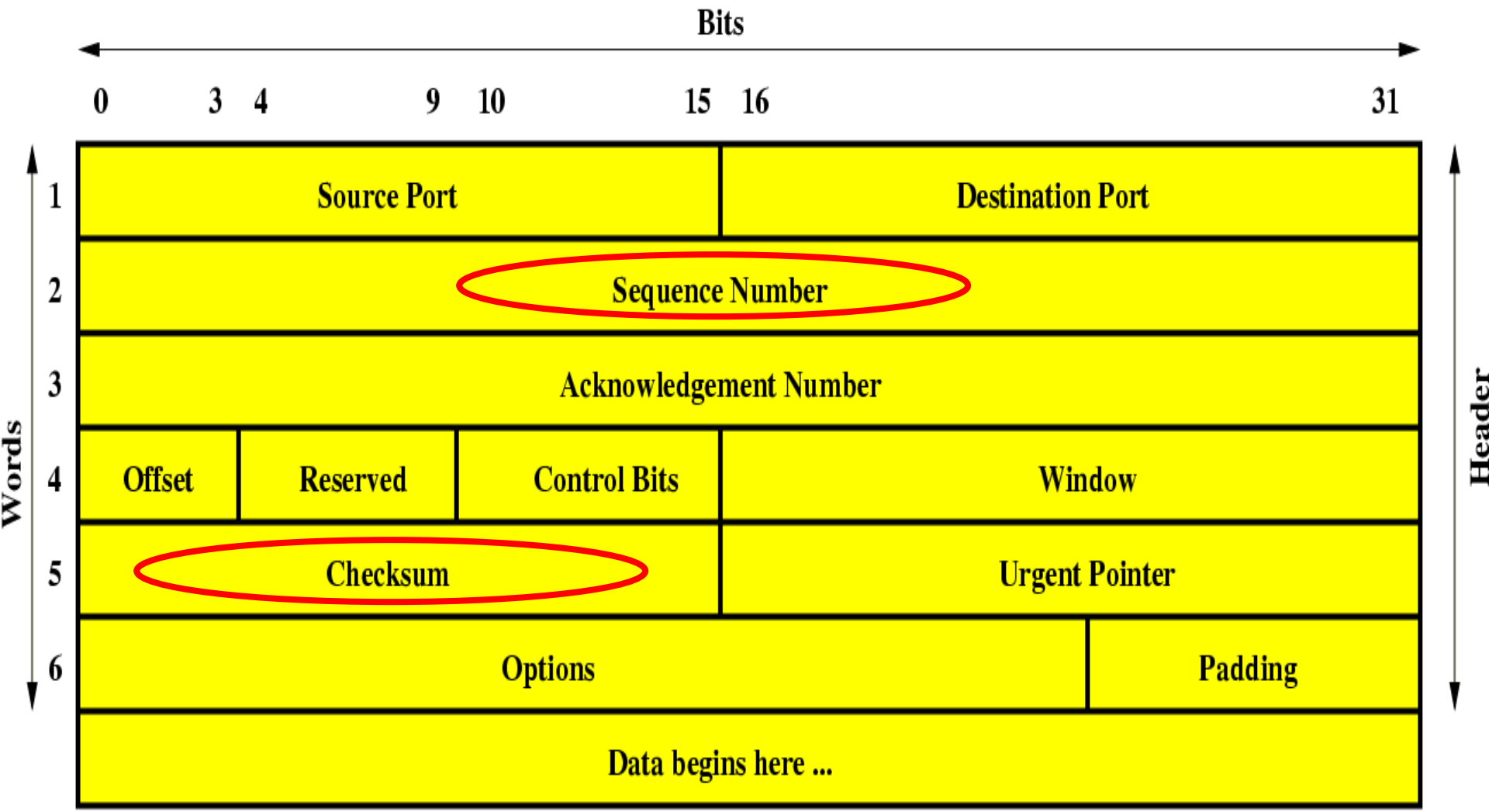
https://en.wikipedia.org/wiki/Checksum

The Transport Layer

- The **transport layer** is responsible for ensuring that:
  - Packets are received in the order they were sent
  - No data is lost or corrupted.
    - If a packet is lost, the transport layer can ask the sender to re-transmit the packet.

- IP networks implement this by adding an additional header to each datagram that contains more information

TCP Packet Format



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																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0				NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
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 segment 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)

The Transport Layer

- There are two primary protocols at this level:
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)

TCP

- **TCP** (Transmission Control Protocol) is a connection-based protocol that provides a reliable flow of data between two computers.
- As a reliable protocol, it allows for retransmission of lost or corrupted data and delivery of bytes in the order they were sent.

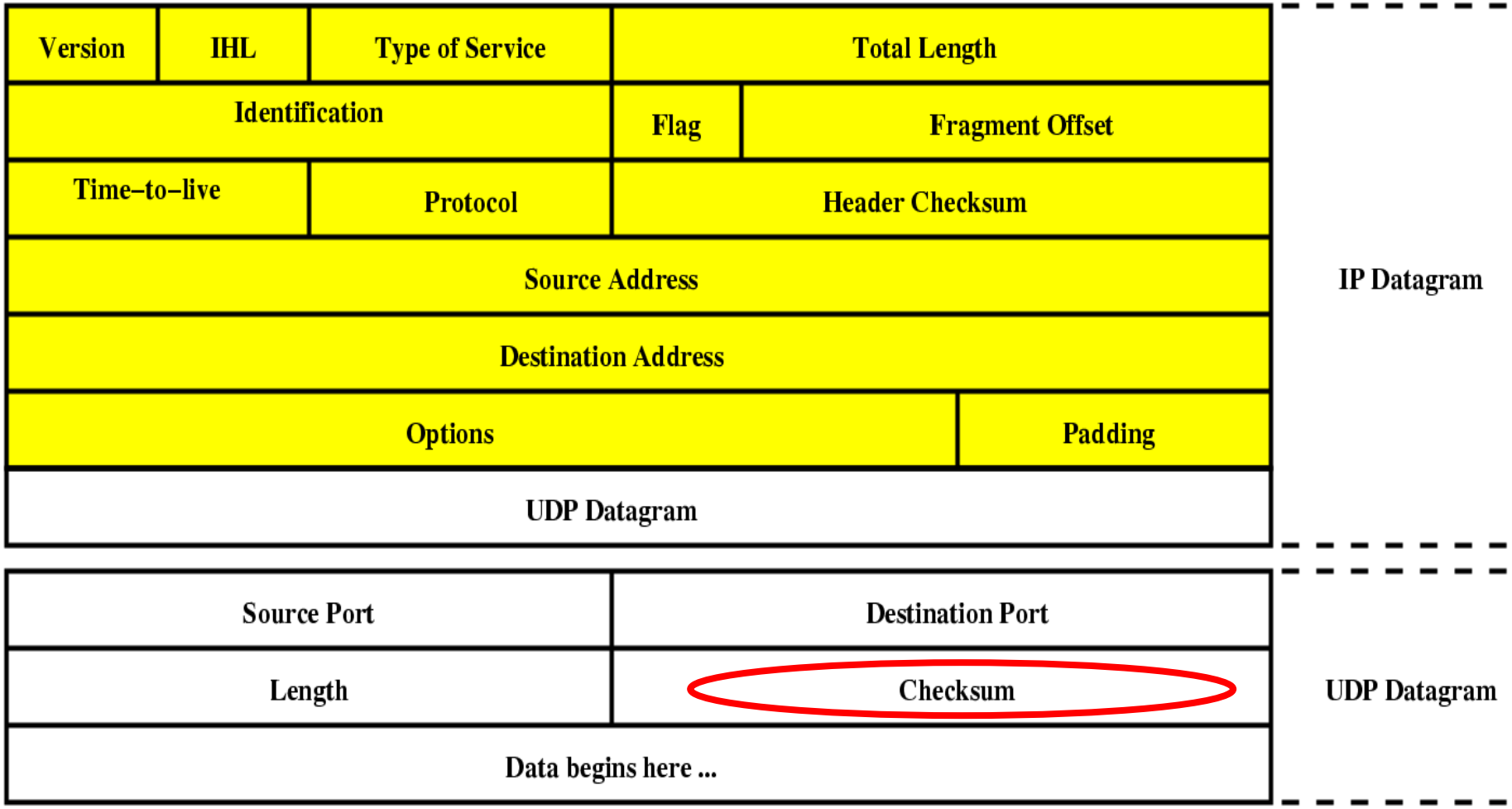
TCP

- As a reliable connection-based, when two applications want to communicate to each other reliably, they establish a connection and send data back and forth over that connection.
  - TCP guarantees that data sent from one end of the connection actually gets to the other end and in the same order it was sent. Otherwise, an error is reported.
  - TCP provides a point-to-point channel for applications that require reliable communications.
    - The Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Telnet are all examples of applications that require a reliable communication channel.
    - When HTTP is used to read from a URL, the data must be received in the order in which it was sent.

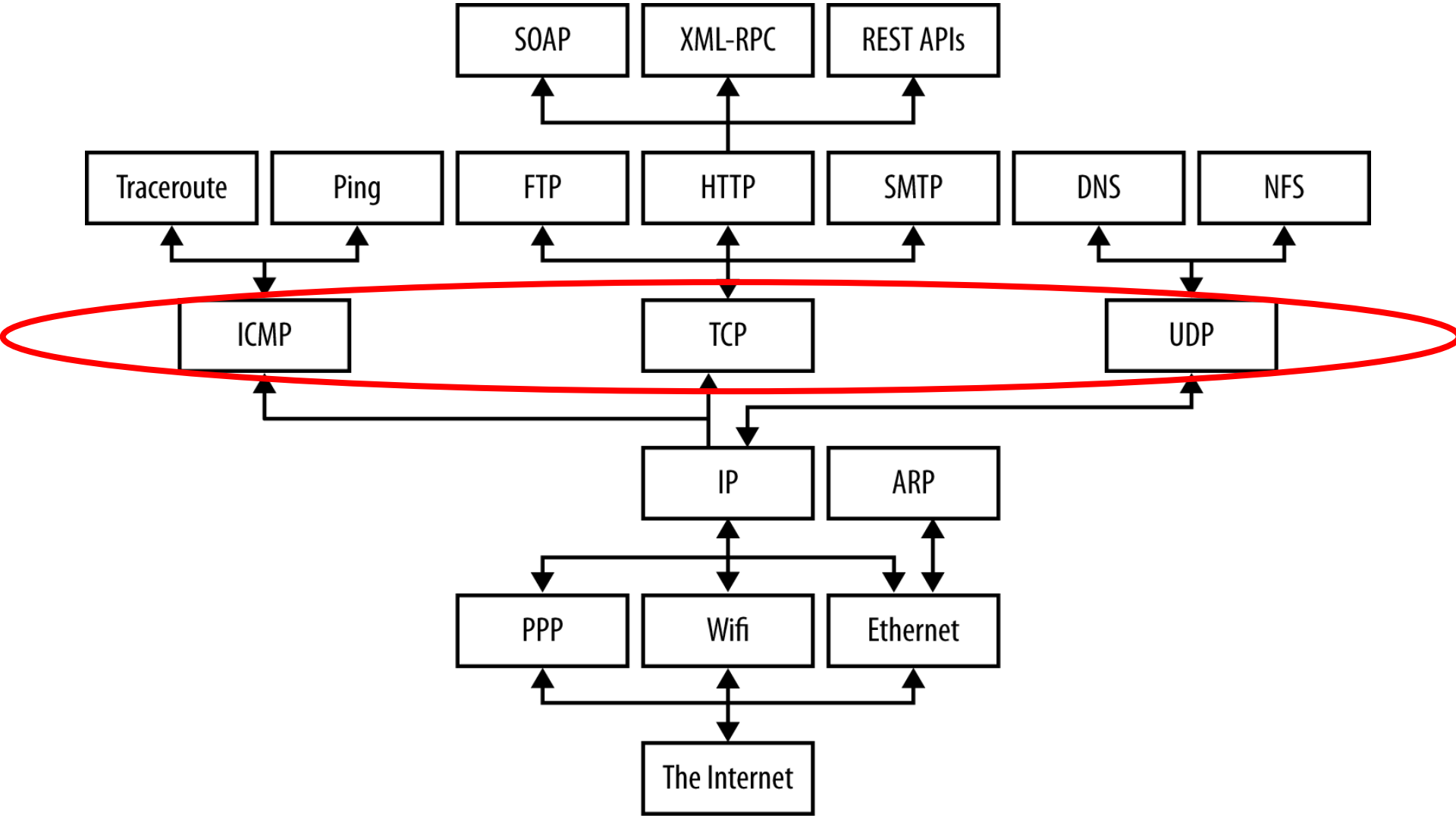
UDP

- **UDP** (User Datagram Protocol) is a protocol that sends independent packets of data, also called datagrams, from one computer to another with no guarantees about arrival.
  - UDP is not connection-based like TCP.
  - Sending datagrams is much like sending a letter through the postal service: The order of delivery is not guaranteed, and each message is independent of any other.
  - **Unreliable.** It's a so-called **best-effort** protocol. (Just like IP)
  - It allows the receiver to detect corrupted packets but does not guarantee that packets are delivered in the correct order, or at all.

UDP Datagram Format



Protocols


SOAP
XML-RPC
REST APIs
Traceroute
Ping
FTP
HTTP
SMTP
DNS
NFS
ICMP
TCP
UDP
IP
ARP
PPP
Wifi
Ethernet
The Internet

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here

Internet Control Message Protocol

From Wikipedia, the free encyclopedia

This article is about the protocol as used with Internet Protocol version 4. For the protocol as used with Internet Protocol version 6, see ICMPv6.

The **Internet Control Message Protocol** (**ICMP**) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.[1] ICMP 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 IPv4 is defined in RFC 792.

Contents [hide]

Internet protocol suite

Application layer

BGP · DHCP · DNS · FTP · HTTP · IMAP · LDAP · MGCP · MQTT · NNTP · NTP · POP · ONC/RPC · RTP · RTSP · RIP · SIP · SMTP · SNMP · SSH · Telnet · TLS/SSL · XMPP ·

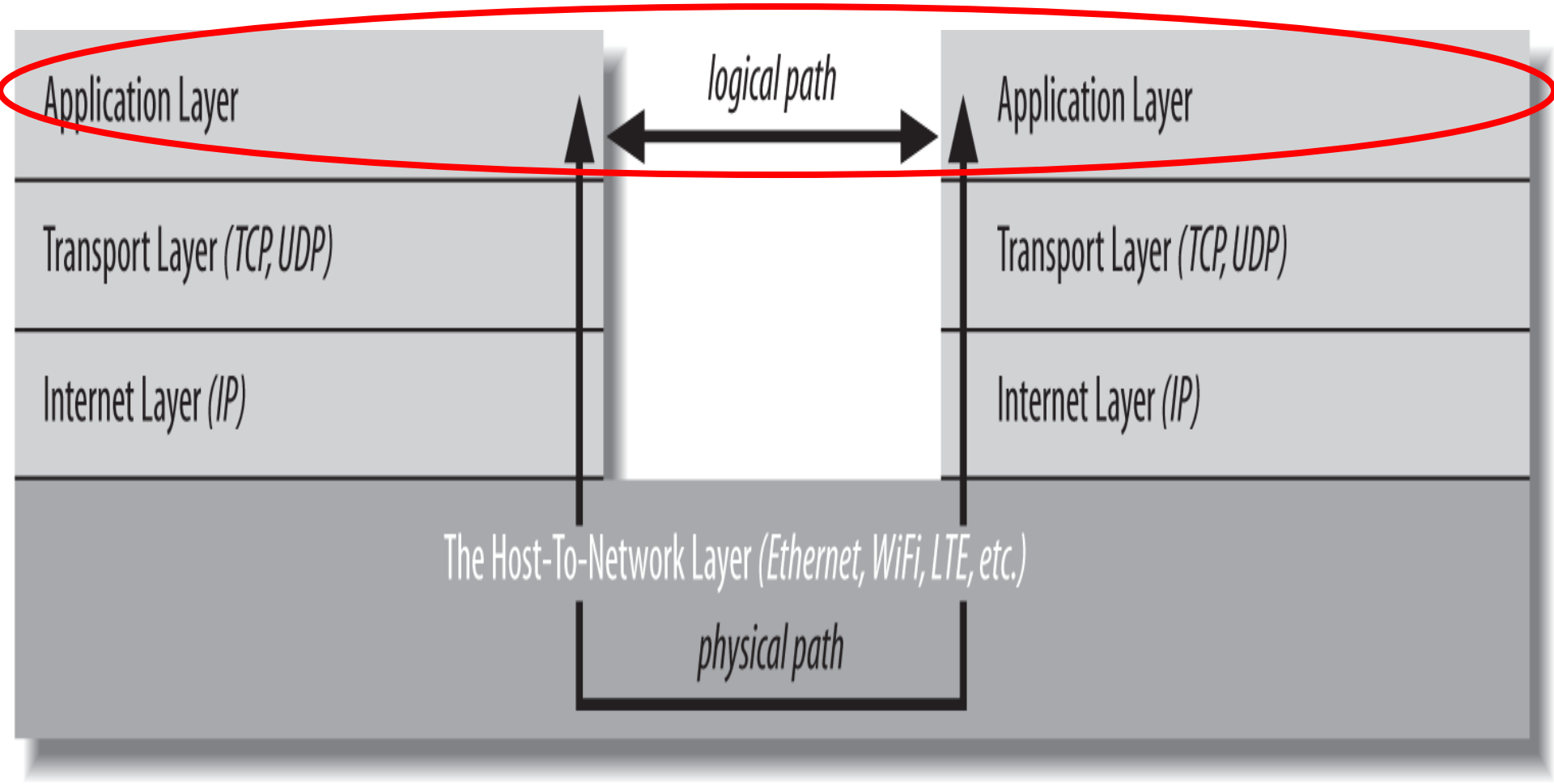
Quiz

- Why would anybody use UDP when TCP is available??

1.6 Exercises

3. IP is a best-effort protocol, requiring that information be broken down into datagrams, which may be lost, duplicated, or reordered. TCP hides all of this, providing a reliable service that takes and delivers an unbroken stream of bytes. How might you go about providing TCP service on top of IP? Why would anybody use UDP when TCP is available?

The TCP/IP 4-Layer Model



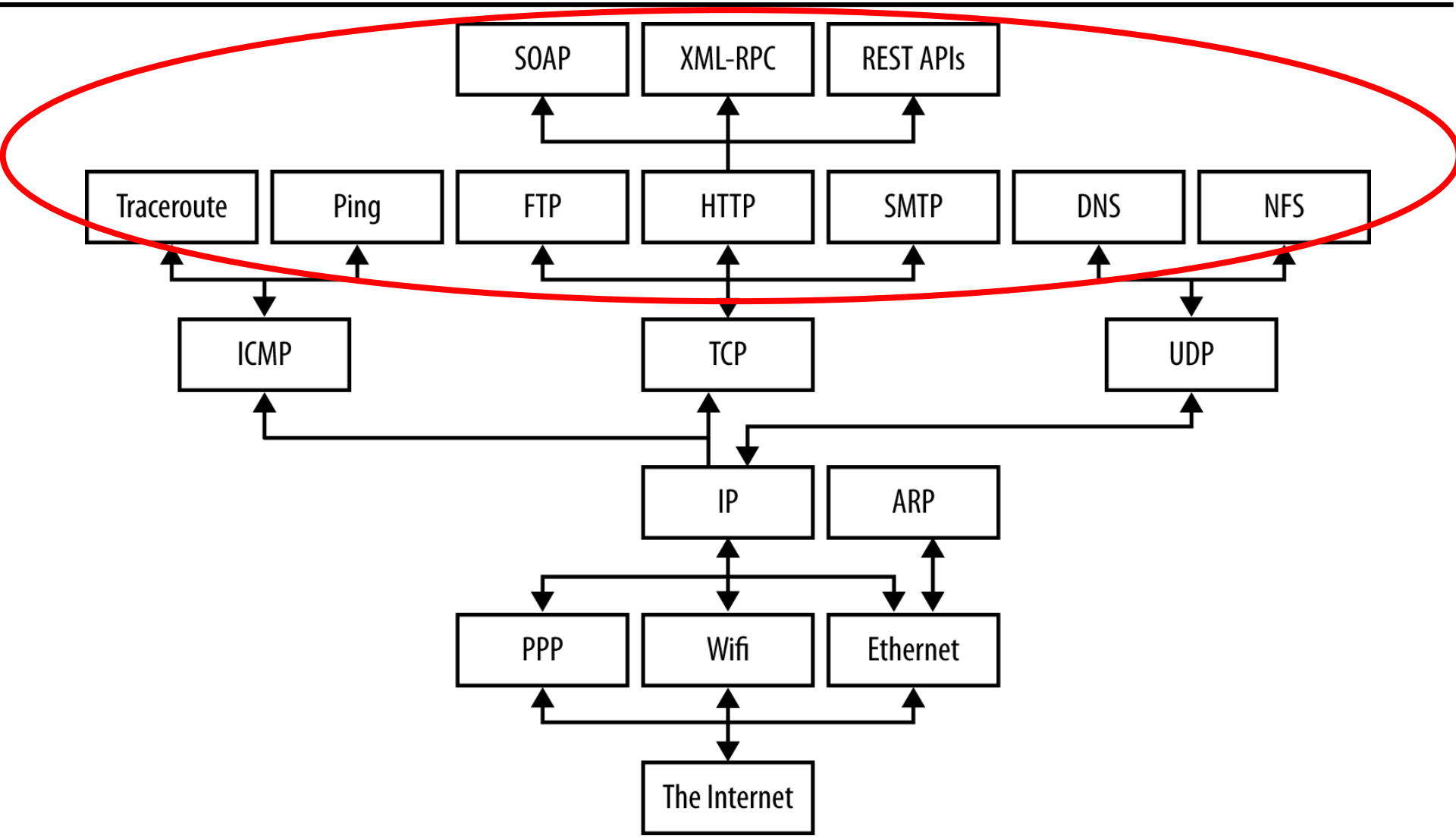
The Application Layer

- The layer that delivers data to the user is called the **application layer**.
  - The three lower layers all work together to define how data is transferred from one computer to another.
  - The application layer decides what to do with the data after it's transferred.
    - For example, HTTP makes sure that your web browser displays a graphic image as a picture, not a long stream of numbers.

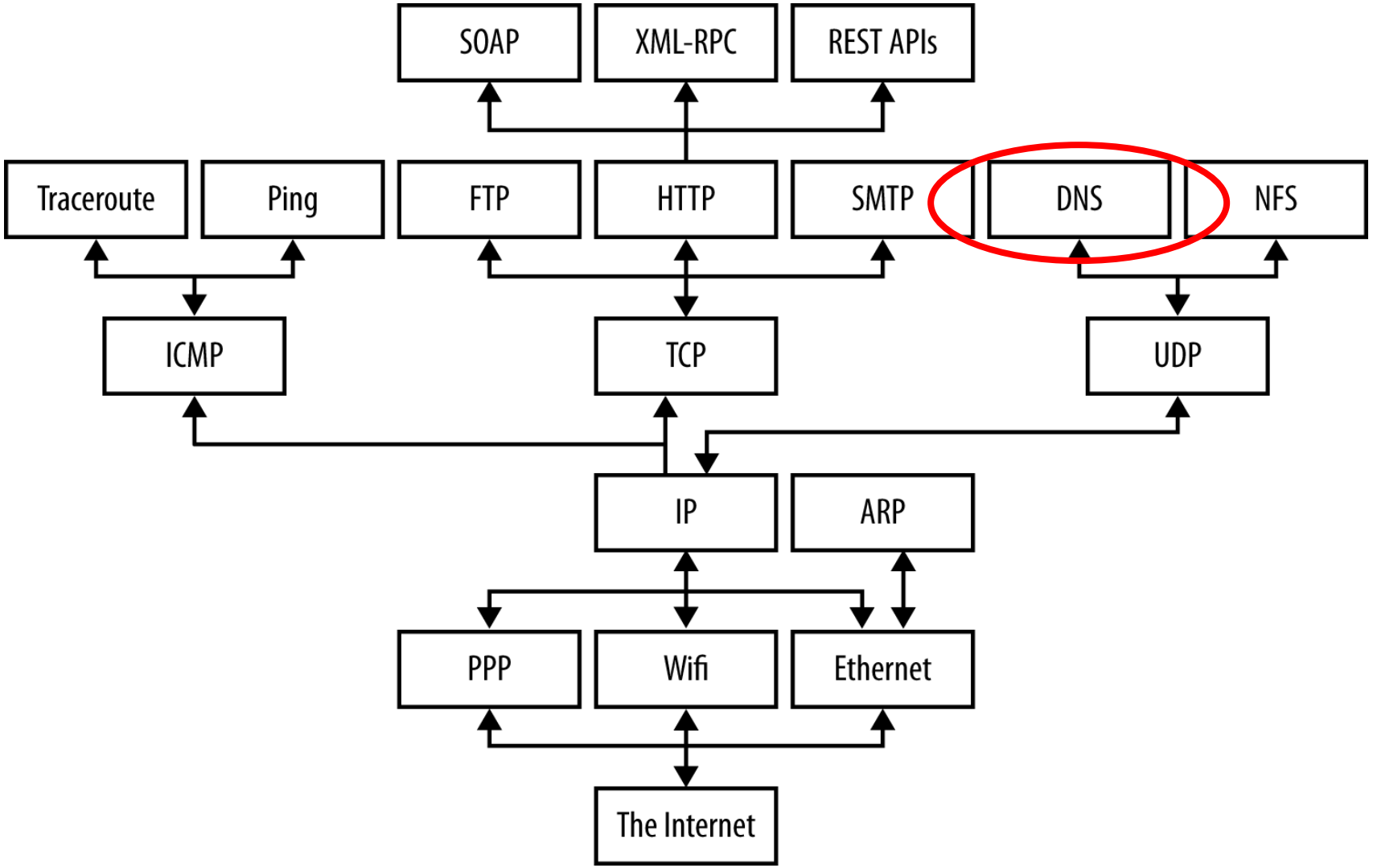
The Application Layer

- There is an entire alphabet soup of application layer protocols:
  - HTTP for the Web
  - SMTP, POP, and IMAP for email
  - FTP, FSP, and TFTP for file transfer
  - NFS for remote file access
  - Gnutella and BitTorrent for file sharing
  - Skype for voice communication
- Your programs can also define their own application layer protocols

Protocols


SOAP
XML-RPC
REST APIs
Traceroute
Ping
FTP
HTTP
SMTP
DNS
NFS
ICMP
TCP
UDP
IP
ARP
PPP
Wifi
Ethernet
The Internet

Protocols


SOAP
XML-RPC
REST APIs
Traceroute
Ping
FTP
HTTP
SMTP
DNS
NFS
ICMP
TCP
UDP
IP
ARP
PPP
Wifi
Ethernet
The Internet

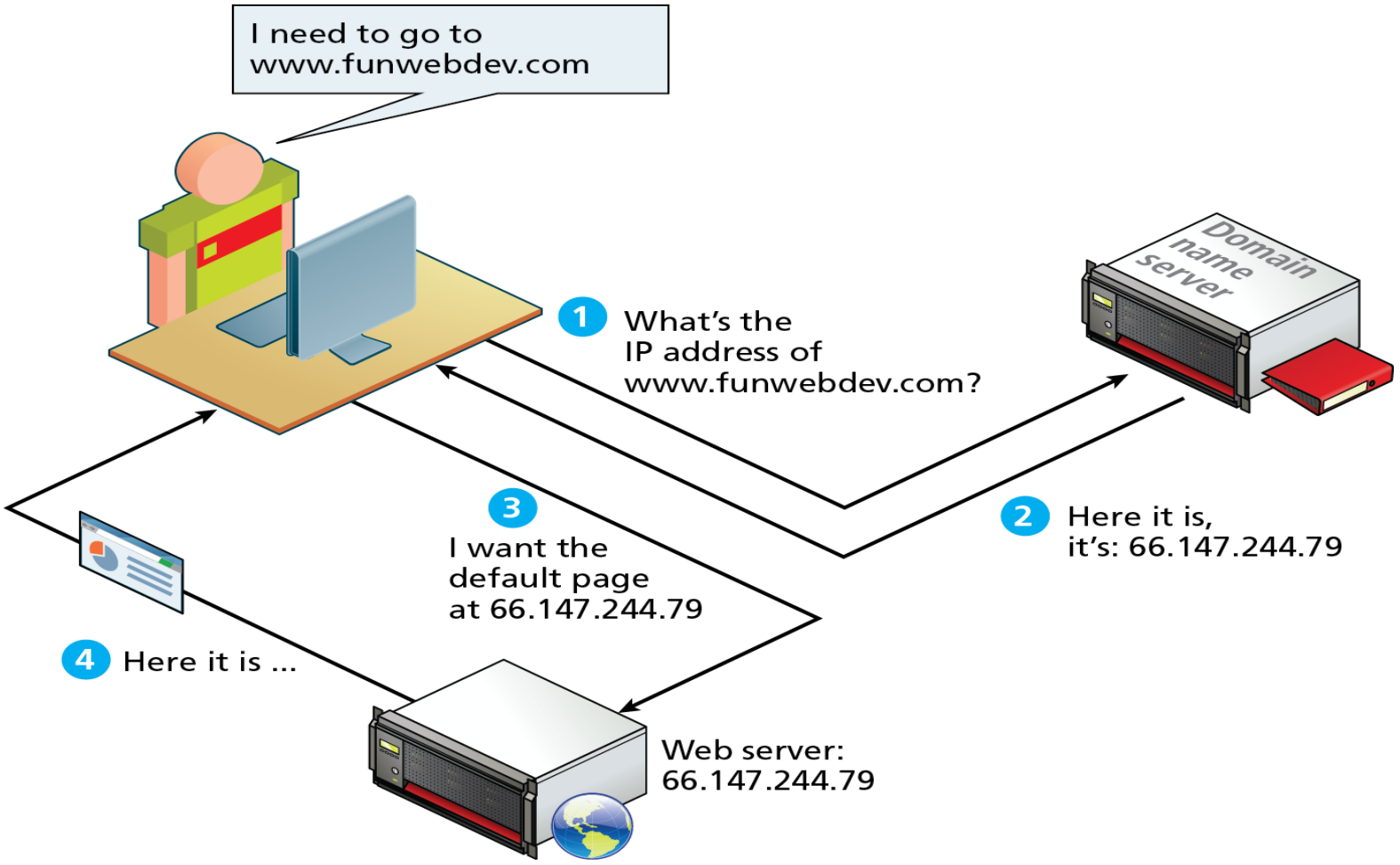
Domain Name Systems

- Although computers are very comfortable with numbers, human beings aren't very good at remembering them.
  - Therefore, the **Domain Name System** (DNS) was developed to translate hostnames that humans can remember:

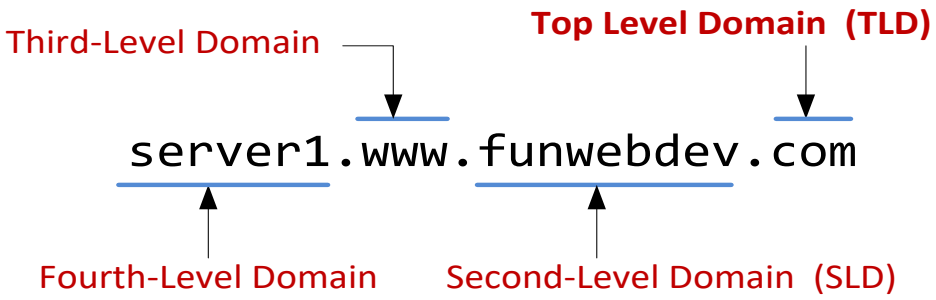
    128.230.171.184 → www.syr.edu

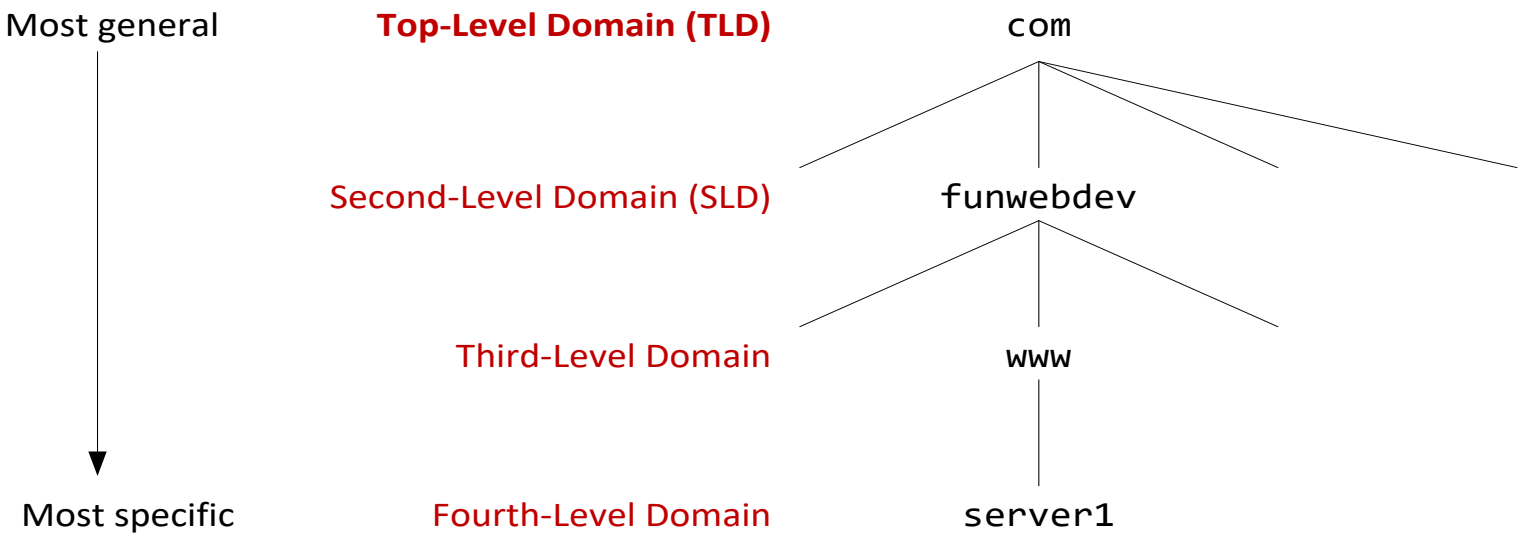
    "www.syr.edu" → 128.230.171.184
  - When Java programs access the network, they need to process both these numeric addresses and their corresponding hostnames.

Domain Name Systems

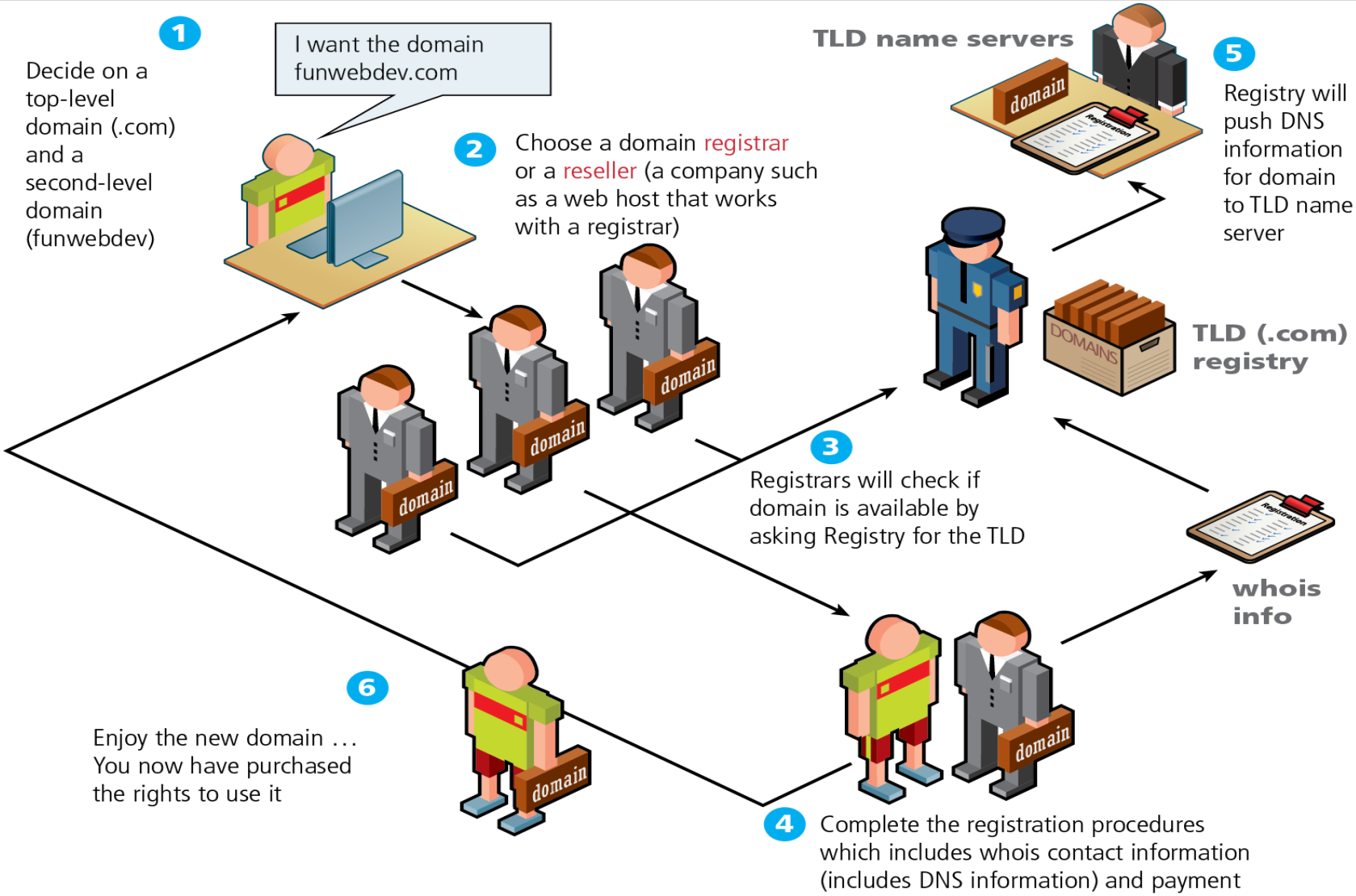


Domain Levels





Domain Name Registration Process



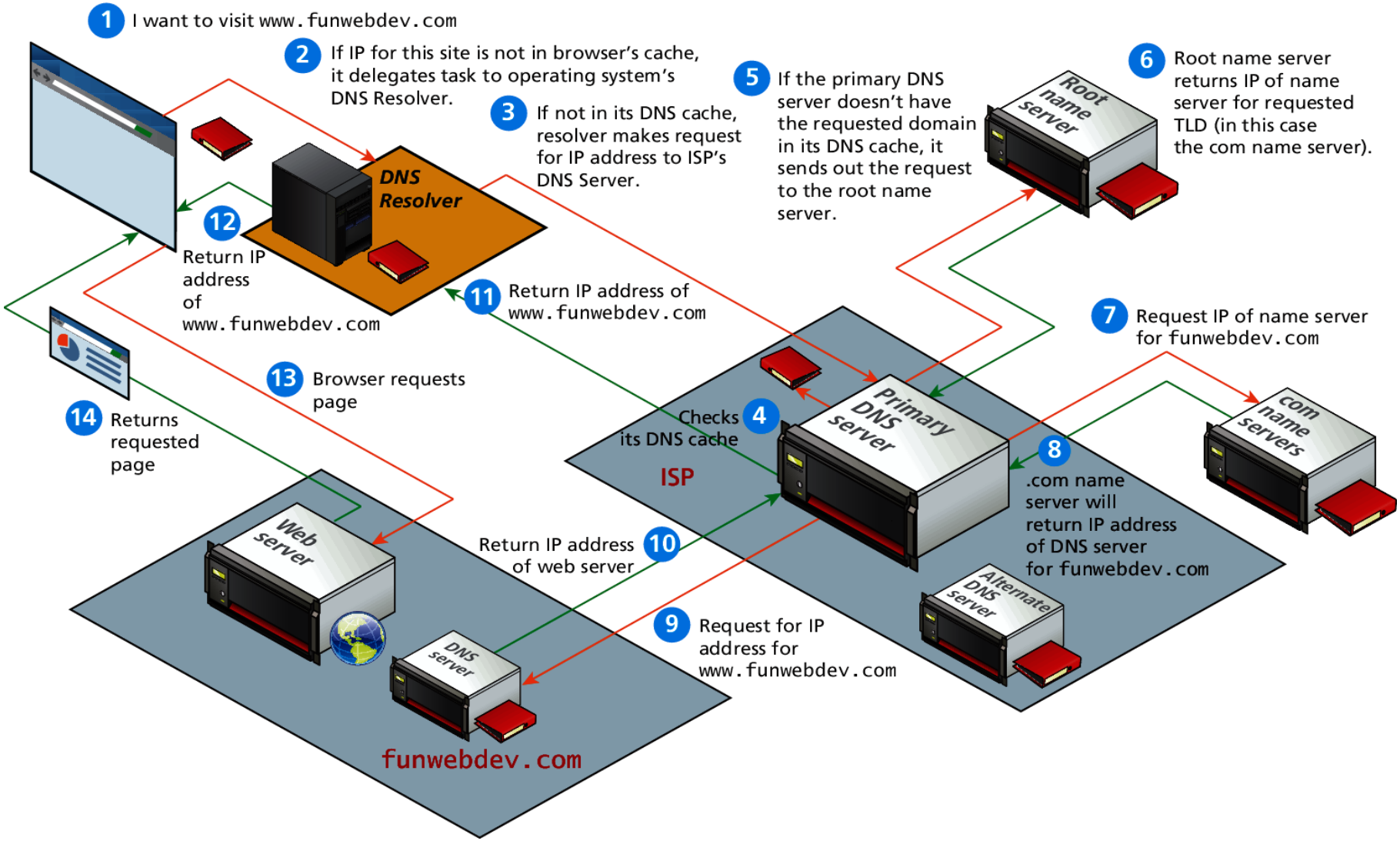
DNS Address Resolution

- While domain names are certainly an easier way for users to reference a web site, eventually, your browser needs to know the IP address of the web site in order to request any resources from it.

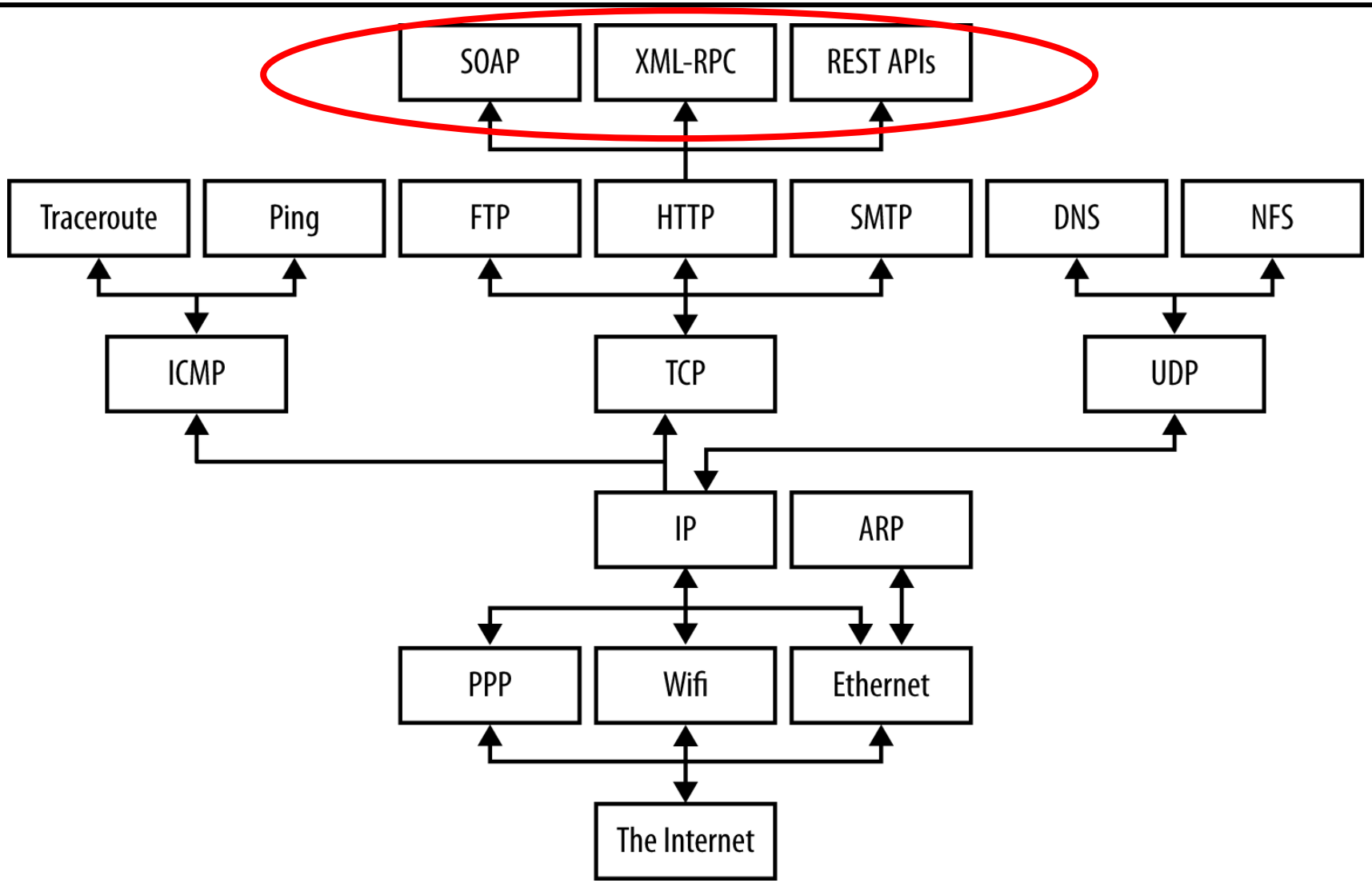
- The Domain Name System provides a mechanism for software to discover this numeric IP address.

- This process is referred to here as **address resolution.**

Domain Name Address Resolution Process



Protocols


SOAP
XML-RPC
REST APIs
Traceroute
Ping
FTP
HTTP
SMTP
DNS
NFS
ICMP
TCP
UDP
IP
ARP
PPP
Wifi
Ethernet
The Internet

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here

SOAP

From Wikipedia, the free encyclopedia

This article is about the computer network protocol. For surfactants used for cleaning, see Soap. For other uses, see Soap (disambiguation).

This article's **lead section does not adequately summarize key points of its contents**. Please consider expanding the lead to provide an accessible overview of all important aspects of the article. Please discuss this issue on the article's talk page. *(June 2012)*

SOAP (originally **Simple Object Access Protocol**) is a protocol specification for exchanging structured information in the implementation of web services in computer networks. Its purpose is to induce extensibility, neutrality and independence. It uses XML Information Set for its message format, and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission.

SOAP allows processes running on disparate operating systems (such as Windows and Linux) to communicate using Extensible Markup Language (XML). Since Web protocols like HTTP are installed and running on all operating systems, SOAP allows clients to invoke web services and receive responses independent of language and platforms.

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here

XML-RPC

From Wikipedia, the free encyclopedia
(Redirected from Xml-rpc)

This article **needs additional citations for verification**. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed. *(October 2016) (Learn how and when to remove this template message)*

XML-RPC is a remote procedure call (RPC) protocol which uses XML to encode its calls and HTTP as a transport mechanism.[1] "XML-RPC" also refers generically to the use of XML for remote procedure call, independently of the specific protocol. This article is about the protocol named "XML-RPC".

Contents [hide]

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link

Representational state transfer

From Wikipedia, the free encyclopedia

"REST" redirects here. For other uses, see REST (disambiguation).

Representational state transfer (**REST**) or **RESTful** web services are a way of providing interoperability between computer systems on the Internet. REST-compliant Web services allow requesting systems to access and manipulate textual representations of Web resources using a uniform and predefined set of stateless operations. Other forms of Web services exist which expose their own arbitrary sets of operations such as WSDL and SOAP.[1]

"Web resources" were first defined on the World Wide Web as documents or files identified by their URLs, but today they have a much more generic and abstract definition encompassing every thing or entity that can be identified, named, addressed or handled, in any way whatsoever, on the Web. In a RESTful Web service, requests made to a resource's URI will elicit a response that may be in XML, HTML, JSON or some other defined format. The response may confirm that some alteration has been made to the stored resource, and it may provide hypertext links to other related resources or collections of resources. Using HTTP, as is most common, the kind of operations available include those predefined by the CRUD HTTP methods GET, POST, PUT, DELETE and so on.

By using a stateless protocol and standard operations, REST systems aim for fast performance, reliability, and the ability to grow, by re-using components that can be managed and updated without affecting the system as a whole, even while it is running.

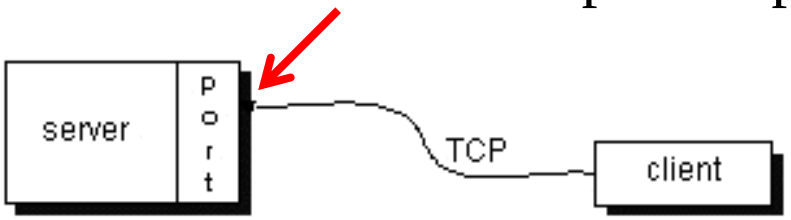
The term *representational state transfer* was introduced and defined in 2000 by Roy Fielding in his doctoral dissertation.[2][3] Fielding's dissertation explained the REST principles were known as the "HTTP object model" beginning in 1994, and

Ports

- Usually, a computer has a single physical connection to the network.
  - All data destined for a particular computer arrives through that connection.
- However, the data may be intended for different applications running on the computer.
  - How does the computer know to which application to forward the data?
    - Through the use of **ports**.

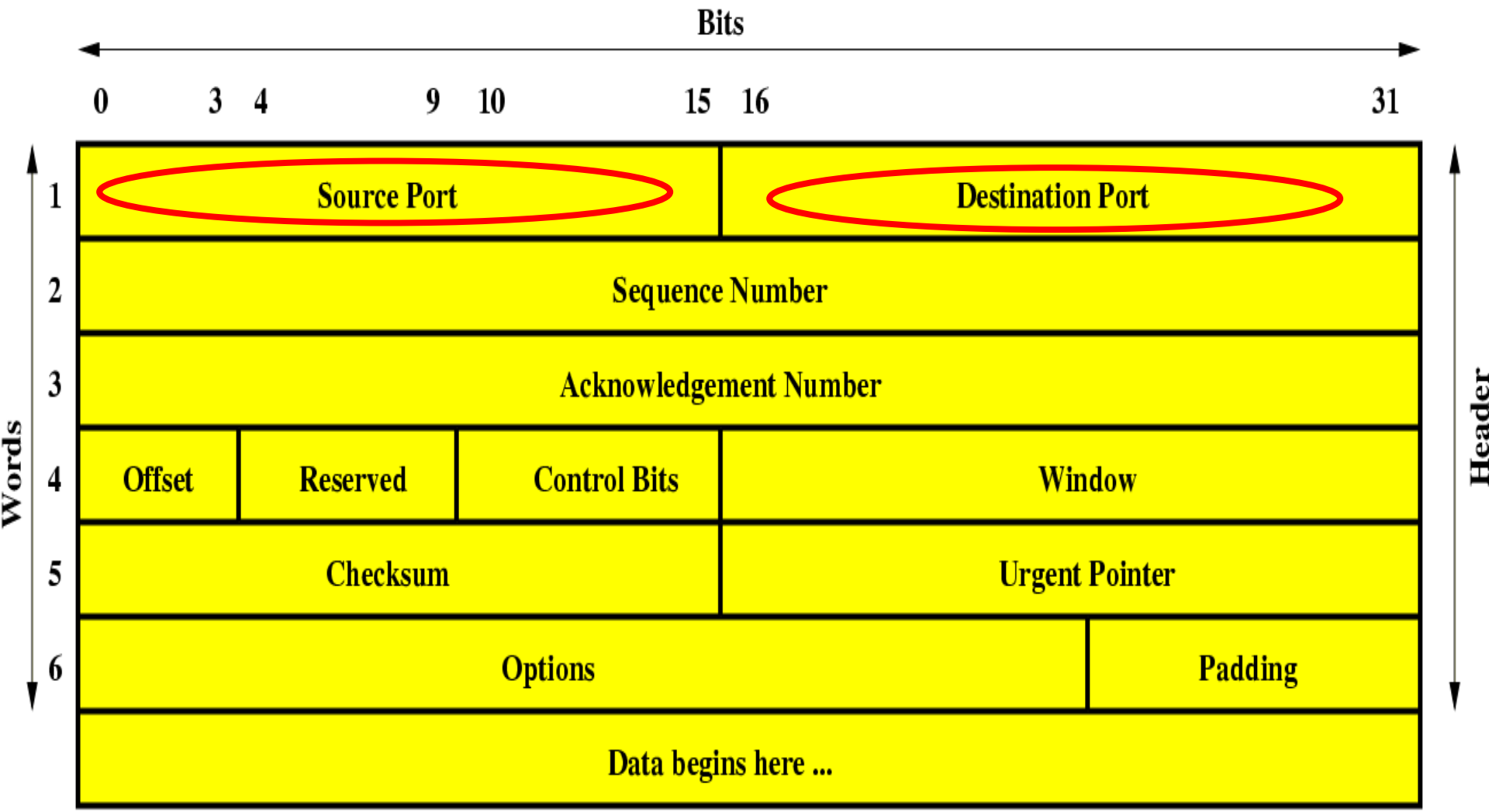
Ports

- Ports are identified by a **16**-bit number, which TCP and UDP use to deliver the data to the right application.
  - In connection-based communication such as TCP, a server application binds a **socket** to a specific port number.

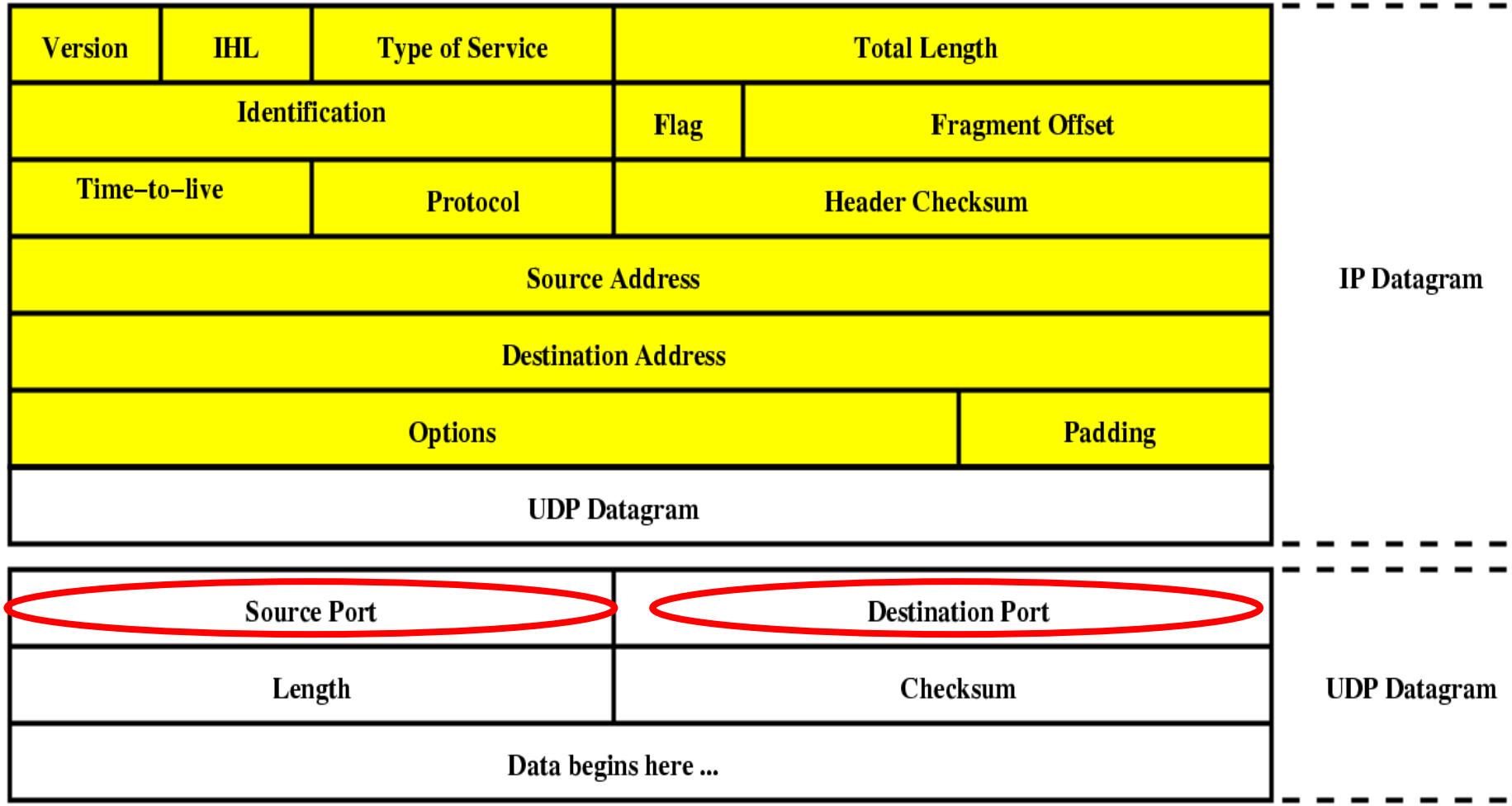


  - This has the effect of registering the server with the system to receive all data destined for that port.
  - A client can then rendezvous with the server at the server's port.

TCP Packet Format

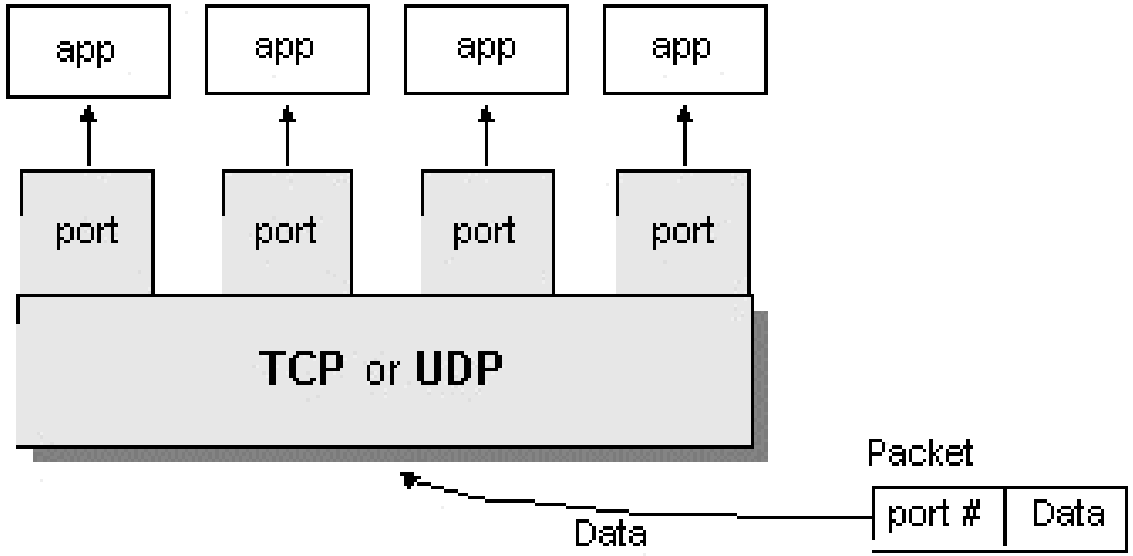


UDP Datagram Format



Ports

- In datagram-based communication such as UDP, the datagram packet contains the port number of its destination and UDP routes the packet to the appropriate application:



Ports

- The port numbers ranging from 0 - 1023 are restricted
  - They are reserved for use by **well-known services** such as HTTP and FTP and other system services.
  - These ports are called **well-known ports**.
  - Your applications should not attempt to bind to them.

Services	Port Numbers
HTTP	80
FTP	21
TELNET	23
POP3	110
SMTP	25

Protocol	Port	Protocol	Purpose
FTP	21	TCP	This port is used to send FTP commands like `put` and `get`.
SSH	22	TCP	Used for encrypted, remote logins.
Telnet	23	TCP	Used for interactive, remote command-line sessions.
smtp	25	TCP	The Simple Mail Transfer Protocol is used to send email between machines.
time	37	TCP/UDP	A time server returns the number of seconds that have elapsed on the server since midnight, January 1, 1900, as a four-byte, unsigned, big-endian integer.
whois	43	TCP	A simple directory service for Internet network administrators.
finger	79	TCP	A service that returns information about a user or users on the local system.
HTTP	80	TCP	The underlying protocol of the World Wide Web.
POP3	110	TCP	Post Office Protocol version 3 is a protocol for the transfer of accumulated email from the host to sporadically connected clients.
NNTP	119	TCP	Usenet news transfer; more formally known as the "Network News Transfer Protocol."
IMAP	143	TCP	Internet Message Access Protocol is a protocol for accessing mailboxes stored on a server.
dict	2628	TCP	A UTF-8 encoded dictionary service that provides definitions of words.

List of TCP and UDP port numbers

From Wikipedia, the free encyclopedia

This is a list of Internet socket port numbers used by protocols of the Transport Layer of the Internet Protocol Suite for the establishment of host-to-host communications.

Originally, these ports number were used by the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP), but are also used for the Stream Control Transmission Protocol (SCTP), and the Datagram Congestion Control Protocol (DCCP). SCTP and DCCP services usually use a port number that matches the service of the corresponding TCP or UDP implementation if they exist. The Internet Assigned Numbers Authority (IANA) is responsible for maintaining the official assignments of port numbers for specific uses.[1] However, many unofficial uses of both well-known and registered port numbers occur in practice.

Contents [hide]

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikimedia Shop

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia

Toolbox

Print/export

Languages
Català