Charlemagne Mendoza

# Computer Networking Essentials

Delve Publishing

# COMPUTER NETWORKING ESSENTIALS

*Editor:*

**Charlemagne Mendoza**




www.bibliotex.com

**Computer Networking Essentials**

*Charlemagne Mendoza*

**www.bibliotex.com**

**email: info@bibliotex.com**

e-book Edition 2018

ISBN: 978-1-98460-897-0 (e-book)

This book contains information obtained from highly regarded resources. Reprinted material sources are indicated. Copyright for individual articles remains with the authors as indicated and published under Creative Commons License. A Wide variety of references are listed. Reasonable efforts have been made to publish reliable data and views articulated in the chapters are those of the individual contributors, and not necessarily those of the editors or publishers. Editors or publishers are not responsible for the ac curacy of the information in the published chapters or consequences of their use. The publisher assumes no responsibility for any damage or grievance to the persons or property arising out of the use of any materials, instructions, methods or thoughts in the book. The editors and the publisher have at- tempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission has not been obtained. If any copyright holder has not been acknowledged, please write to us so we may rectify.

**Notice**: Registered trademark of products or corporate names are used only for explanation and identification without intent of infringement.

**© 2017 Delve Publishing**

In Collaboration with Delve Publishing. Originally Published in printed book format by Delve Publishing with ISBN 978-1-68095-671-9



# About the Editor

## Charlemagne Mendoza

Charlemagne acquired his Bachelor's degree at the University of Caloocan City in 2012, He is an IT enthusiast that focuses on real-world innovations using information systems in multiple platforms. He is the current CEO for Carlo Solutions a Philippine based company that delivers Sales and Marketing improvement through the use of information systems.

# Table of Contents

List of Abbreviations ..... xi
*Preface* ..... xiii

## 1 COMPUTER NETWORK: AN INTRODUCTION

Introduction ..... 1
History ..... 2
Properties ..... 3
Network Packet ..... 3
Network Topology ..... 4
Communications Protocols ..... 12
Organizational Scope ..... 17
Routing ..... 19
Network Service ..... 20
Network Performance ..... 20
Security ..... 21
Views of Networks ..... 23
References ..... 24

## 2 HISTORY OF THE INTERNET

Introduction ..... 27
Precursors ..... 28
Development of Wide-Area Networking ..... 29
Networks that Led to the Internet ..... 30
Cyclades ..... 32
TCP/IP Goes Global (1980s) ..... 38
Internet Governance ..... 47
Politicization of the Internet ..... 50
Use and Culture ..... 52
Web Technologies ..... 56

Historiography ..... 57
References ..... 57

# 3 NETWORK PACKET

Introduction ..... 67
Terminology ..... 68
Packet Framing ..... 68
Example: IP Packets ..... 69
Example: The Nasa Deep Space Network ..... 70
Example: Radio and TV Broadcasting ..... 71
References ..... 74

# 4 NETWORK TOPOLOGY

Introduction ..... 75
Topology ..... 76
Classification ..... 76
Centralization ..... 81
Decentralization ..... 82
Local Area Network ..... 83
Cabling ..... 84
Wireless Media ..... 84
Technical Aspects ..... 85
Metropolitan Area Network ..... 85
Wide Area Network ..... 85
Design Options ..... 86
Connection Technology ..... 87
Asynchronous Transfer Mode ..... 87
Layer 2 – Datagrams ..... 89
Deployment ..... 95
Wireless ATM or Mobile ATM ..... 95
Cable Modem ..... 96
IEEE 802.7 ..... 97
Multimedia Terminal Adapter ..... 100
Network Architectural Functions ..... 100
Cable Modem Flap ..... 101
Dial-Up Internet Access ..... 101
Availability ..... 102
Replacement by Broadband ..... 102
Performance ..... 103
Leased Line ..... 105

Applications ..... 106
Availability ..... 107
Leased Line Alternatives ..... 108
Software-Defined Networking ..... 108
Concept ..... 111
The Need for a New Network Architecture ..... 111
Architectural Components ..... 113
SDN Control Plane ..... 114
Sdn Flow Forwarding (SDN) ..... 115
Applications ..... 115
References ..... 117

# 5 NETWORK PROTOCOLS

List Of Network Protocols ..... 123
WI-FI ..... 124
Etymology ..... 125
Wi-Fi Certification ..... 126
IEEE 802.11 Standard ..... 127
Uses ..... 127
Wi-Fi radio Spectrum ..... 130
Service Set Identifier (SSID) ..... 131
Throughput ..... 131
Hardware ..... 132
Range ..... 136
Multiple Access Points ..... 138
Network Security ..... 138
List of Bluetooth Protocols ..... 138
Controller Stack ..... 139
Host Stack ..... 141
Routing Protocol ..... 143
OSI Layer Designation ..... 144
Interior Gateway Protocols ..... 144
File Transfer Protocol ..... 144
Web Browser Support ..... 148
Transmission Control Protocol ..... 148
Network Function ..... 148
Hypertext Transfer Protocol ..... 149
Technical Overview ..... 150
Request Methods ..... 152
Network Time Protocol ..... 155
Clock Strata ..... 156

Stratum 0 ..... 157
Stratum 1 ..... 157
Stratum 2 ..... 157
Stratum 3 ..... 157
Timestamps ..... 158
Clock Synchronization Algorithm ..... 158
Software Implementations ..... 159
References ..... 160

# 6 ETHERNET

Introduction ..... 171
Standardization ..... 174
Evolution ..... 175
Varieties of Ethernet ..... 181
Frame Structure ..... 181
Autonegotiation ..... 182
Electrical Signals ..... 183
The Base Link Code Word ..... 184
Message and Unformatted Next Page ..... 185
Priority ..... 185
Interoperability Problems ..... 186
Duplex Mismatch ..... 186
Patents ..... 187
References ..... 187

# 7 ARPANET

Introduction ..... 191
Software and Protocols ..... 199
Arpanet in Popular Culture ..... 200
Bitnet ..... 201
Technical Details ..... 201
Extent ..... 202
Legacy ..... 202
Cellular Network ..... 202
Concept ..... 203
Cell Signal Encoding ..... 204
Frequency Reuse ..... 205
Directional Antennas ..... 206
Movement from Cell to Cell and Handing Over ..... 207
Mobile Phone Network ..... 208

Cyclades ..... 211
Conception and Deployment ..... 211
Technical Details ..... 212
Demise ..... 212
Legacy ..... 213
References ..... 213

# 8 TELECOMMUNICATIONS EQUIPMENT

Introduction ..... 217
Types ..... 217
Analogue Switch ..... 218
Transmission Line ..... 219
Applicability ..... 219
The Four Terminal Model ..... 220
Communications satellite ..... 221
Satellite Orbits ..... 222
Structure ..... 226
Frequency Allocation for Satellite Systems ..... 226
Applications ..... 227
Modem ..... 230
Dialup Modem ..... 231
Router (Computing) ..... 245
Applications ..... 246
Historical and Technical Information ..... 249
Forwarding ..... 250
References ..... 251

# 9 WORLD WIDE WEB

Introduction ..... 255
History Of The World Wide Web ..... 258
Precursors ..... 258
1980–1991: Invention and Implementation of the Web ..... 259
1992–1995: Growth of the Web ..... 260
1996–1998: Commercialization of the Web ..... 262
1999–2001: “Dot-Com” Boom and Bust ..... 262
2002–Present: The Web Becomes Ubiquitous ..... 263
Function ..... 267
Web Security ..... 271
Privacy ..... 272
Standards ..... 272

Accessibility ..... 273
Internationalization ..... 273
Statistics ..... 274
Speed Issues ..... 274
Web Caching ..... 274
References ..... 275

Index ..... 281

# List of Abbreviations

| | |
|---|---|
| ARPA | Advanced Research Projects Agency |
| ARPANET | Advanced Research Projects Agency Network |
| DTN | Delay-tolerant networking |
| DMC | Direct Multiplex Control |
| DNS | Domain Name System |
| BBN | Bolt, Beranek and Newman |
| BSS | Broadcasting satellite service |
| BTV | business television |
| B2B | business-to-business |
| B2C | business-to-consumer |
| CAN | campus area network |
| CSMA/CD | carrier sense multiple access with collision detection |
| CSNET | Computer Science Network |
| CBR | constant bit rate |
| CCSDS | Consultative Committee for Space Data Systems |
| CRC | cyclic redundancy check |
| DARPA | Defense Advanced Research Projects Agency |
| DTN | Delay-tolerant networking |
| DMC | Direct Multiplex Control |
| FCC | Federal Communications Commission |
| GEO | geostationary orbit |
| HES | Hypertext Editing System |
| HTML | Hypertext Markup Language |

| | |
|---|---|
| HTTP | Hypertext Transfer Protocol |
| ISDN | Integrated Services Digital Network |

# Preface

Computer networking refers to the study and analysis of the communication process among various computing devices or computer systems that are linked or networked, together to exchange information and share resources. Computer networking depends on the theoretical application and practical implementation of fields like computer engineering, computer sciences, information technology and telecommunication. Today the world scenario is changing. Data Communication and network have changed the way business and other daily affair works. Now, they rely on computer networks and internetwork. A set of devices often mentioned as nodes connected by media link is called a Network. A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called Communication channels. Computer network is a telecommunication channel through which we can share our data. It is also called data network. The best example of a computer network is the Internet. Computer network does not mean a system with control unit and other systems as its slave. It is called a distributed system. Computer networks can be broken down historically into topologies, which is a technique of connecting computers. The most common topology today is a collapsed ring. This is due to the success of a network protocol called the Ethernet. This protocol, or a network language, supports the Internet, Local Area Networks, and Wide Area Networks. A router, network card and protocols are the essential pillars upon which any network is built. Computer networks are the backbone of modern-day communication. Even public switched telephone networks are controlled by computer systems; most telephonic services are also working with IP. The increasing scope of communication has led to much advancement in the networking field and in its relative industries like hardware, software manufacturing and integration.

## Content Coverage

*Chapters One* and *Two* focus on network fundamentals and history of the Internet, respectively. The Internet has always been an emerging technology and an emerging ideal.

*Chapters Three and Four* are about network packet and network topology, separately. A packet consists of control information and user data, which is also known

as the payload, whereas network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network

*Chapter Five* focuses on network protocols system that has an ability to withstand changes in a procedure or recover from a range of exceptional inputs and situations in a given environment.

*Chapters Six* and *Seven* present about Ethernet and ARPANET, separately. Ethernet is a standard communications protocol embedded in software and hardware devices, intended for building a local area network, whereas ARPANET implemented the type of packet switching network that would come to dominate communications around the world.

*Chapters Eight* and *Nine* present information about telecommunications equipment and World Wide Web, separately. The Internet encompasses the Web, but it also encompasses other online protocols in addition to the Web.

CHAPTER 1

# Computer Network: An Introduction

## Chapter Contents

- **Introduction**

A computer network is a set of computers connected together for the purpose of sharing resources. The most common resource shared today is the connection to the Internet. Other shared resources can include a printer or a file server.

## INTRODUCTION

A computer network or data network is a telecommunications network which allows nodes to share resources. In computer networks, networked computing devices exchange data with each other using a data link. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks differ in the transmission medium used to carry their signals, communications protocols to organize network traffic, the network's size, topology and organizational intent.

Computer networks support an enormous number of applications and services such as access to the World Wide Web, digital video, digital audio, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications as well as many others. In most cases, application-specific communications protocols are layered (i.e. carried as payload) over other more general communications protocols.

## History

The chronology of significant computer-network developments includes:

- In the late 1950s, early networks of computers included the military radar system Semi-Automatic Ground Environment (SAGE).
- In 1959, Anatolii Ivanovich Kitov proposed to the Central Committee of the Communist Party of the Soviet Union a detailed plan for the re-organization of the control of the Soviet armed forces and of the Soviet economy on the basis of a network of computing centres.
- In 1960, the commercial airline reservation system semi-automatic business research environment (SABRE) went online with two connected mainframes.
- In 1962, J.C.R. Licklider developed a working group he called the "Intergalactic Computer Network", a precursor to the ARPANET, at the Advanced Research Projects Agency (ARPA).
- In 1964, researchers at Dartmouth College developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at Massachusetts Institute of Technology, a research group supported by General Electric and Bell Labs used a computer to route and manage telephone connections.
- Throughout the 1960s, Leonard Kleinrock, Paul Baran, and Donald Davies independently developed network systems that used packets to transfer information between computers over a network.
- In 1965, Thomas Marill and Lawrence G. Roberts created the first wide area network (WAN). This was an immediate precursor to the ARPANET, of which Roberts became program manager.
- Also in 1965, Western Electric introduced the first widely used telephone switch that implemented true computer control.
- In 1969, the University of California at Los Angeles, the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah became connected as the beginning of the ARPANET network using 50 kbit/s circuits.
- In 1972, commercial services using X.25 were deployed, and later used as an underlying infrastructure for expanding TCP/IP networks.
- In 1973, Robert Metcalfe wrote a formal memo at Xerox PARC describing Ethernet, a networking system that was based on the Aloha network, developed in the 1960s by Norman Abramson and colleagues at the University of Hawaii.

In July 1976, Robert Metcalfe and David Boggs published their paper "Ethernet: Distributed Packet Switching for Local Computer Networks" and collaborated on several patents received in 1977 and 1978. In 1979, Robert Metcalfe pursued making Ethernet an open standard.

- In 1976, John Murphy of Datapoint Corporation created ARCNET, a token-passing network first used to share storage devices.
- In 1995, the transmission speed capacity for Ethernet increased from 10 Mbit/s to 100 Mbit/s. By 1998, Ethernet supported transmission speeds of a Gigabit. Subsequently, higher speeds of up to 100 Gbit/s were added (as of 2016). The ability of Ethernet to scale easily (such as quickly adapting to support new fiber optic cable speeds) is a contributing factor to its continued use.

## Properties

Computer networking may be considered a branch of electrical engineering, telecommunications, computer science, information technology or computer engineering, since it relies upon the theoretical and practical application of the related disciplines.

A computer network facilitates interpersonal communications allowing users to communicate efficiently and easily via various means: email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing. Providing access to information on shared storage devices is an important feature of many networks. A network allows sharing of files, data, and other types of information giving authorized users the ability to access information stored on other computers on the network. A network allows sharing of network and computing resources. Users may access and use resources provided by devices on the network, such as printing a document on a shared network printer. Distributed computing uses computing resources across a network to accomplish tasks. A computer network may be used by computer crackers to deploy computer viruses or computer worms on devices connected to the network, or to prevent these devices from accessing the network via a denial of service attack.

## Network Packet

Computer communication links that do not support packets, such as traditional point-to-point telecommunication links, simply transmit data as a bit stream. However, most information in computer networks is carried in *packets*. A network packet is a formatted unit of data (a list of bits or bytes, usually a few tens of bytes to a few kilobytes long) carried by a packet-switched network.

In packet networks, the data is formatted into packets that are sent through the network to their destination. Once the packets arrive they are reassembled into their original message. With packets, the bandwidth of the transmission medium can be better shared among users than if the network were circuit switched. When one user is not sending packets, the link can be filled with packets from other users, and so the cost can be shared, with relatively little interference, provided the link isn't overused.

Packets consist of two kinds of data: control information, and user data (payload). The control information provides data the network needs to deliver the user data, for example: source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers, with payload data in between. Often the route a packet needs to take through a network is not immediately available. In that case the packet is queued and waits until a link is free.

## Network Topology

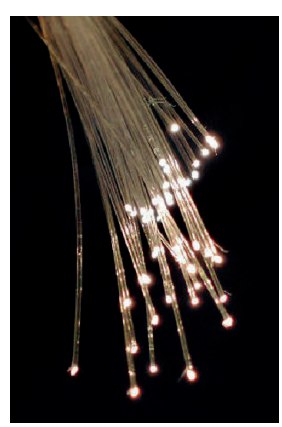
The physical layout of a network is usually less important than the topology that connects network nodes. Most diagrams that describe a physical network are therefore topological, rather than geographic. The symbols on these diagrams usually denote network links and network nodes.

### *Network Links*

The transmission media (often referred to in the literature as the *physical media*) used to link devices to form a computer network include electrical cable (Ethernet, HomePNA, power line communication, G.hn), optical fiber (fiber-optic communication), and radio waves (wireless networking). In the OSI model, these are defined at layers 1 and 2 — the physical layer and the data link layer.

A widely adopted *family* of transmission media used in local area network (LAN) technology is collectively known as Ethernet. The media and protocol standards that enable communication between networked devices over Ethernet are defined by IEEE 802.3. Ethernet transmits data over both copper and fiber cables. Wireless LAN standards (e.g. those defined by IEEE 802.11) use radio waves, or others use infrared signals as a transmission medium. Power line communication uses a building's power cabling to transmit data.

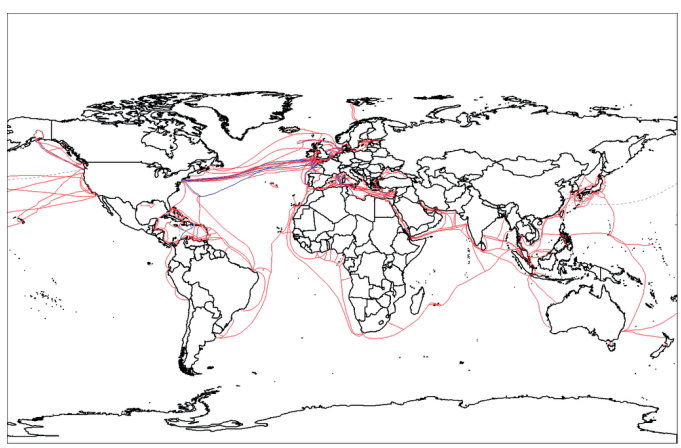
### *Wired Technologies*



Fiber optic cables are used to transmit light from one computer/network node to another

The orders of the following wired technologies are, roughly, from slowest to fastest transmission speed.

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



2007 map showing submarine optical fiber telecommunication cables around the world.

- An *optical fiber* is a glass fiber. It carries pulses of light that represent data. Some advantages of optical fibers over metal wires are very low transmission loss and immunity from electrical interference. Optical fibers can simultaneously carry multiple wavelengths of light, which greatly increases the rate that data can be sent, and helps enable data rates of up to trillions of bits per second. Optic fibers can be used for long runs of cable carrying very high data rates, and are used for undersea cables to interconnect continents.

Price is a main factor distinguishing wired- and wireless-technology options in a business. Wireless options command a price premium that can make purchasing wired computers, printers and other devices a financial benefit. Before making the decision to purchase hard-wired technology products, a review of the restrictions and limitations of the selections is necessary. Business and employee needs may override any cost considerations.

## *Wireless Technologies*



Computers are very often connected to networks using wireless links

- *Terrestrial microwave* – Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low-gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km (30 mi) apart.
- *Communications satellites* – Satellites communicate via microwave radio waves, which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically in geosynchronous orbit 35,400 km (22,000 mi) above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.
- *Cellular and PCS systems* use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.
- *Radio and spread spectrum technologies* – Wireless local area networks use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. IEEE 802.11 defines a common flavor of open-standards wireless radio-wave technology known as Wi-fi.
- *Free-space optical communication* uses visible or invisible light for communications. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices.

## Exotic Technologies

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

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

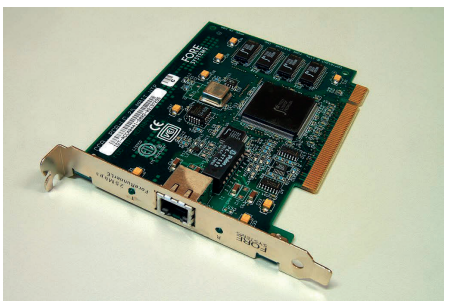
Both cases have a large round-trip delay time, which gives slow two-way communication, but doesn't prevent sending large amounts of information.

## Network Nodes

### Node (networking)

Apart from any physical transmission medium there may be, networks comprise additional basic system building blocks, such as network interface controller (NICs), repeaters, hubs, bridges, switches, routers, modems, and firewalls.

## Network Interfaces



An ATM network interface in the form of an accessory card. A lot of network interfaces are built-in.

A network interface controller (NIC) is computer hardware that provides a computer with the ability to access the transmission media, and has the ability to process low-level network information. For example, the NIC may have a connector for accepting a cable, or an aerial for wireless transmission and reception, and the associated circuitry.

The NIC responds to traffic addressed to a network address for either the NIC or the computer as a whole.

In Ethernet networks, each network interface controller has a unique Media Access Control (MAC) address—usually stored in the controller's permanent memory. To avoid address conflicts between network devices, the Institute of Electrical and Electronics Engineers (IEEE) maintains and administers MAC address uniqueness. The size of an Ethernet MAC address is six octets. The three most significant octets are reserved to

identify NIC manufacturers. These manufacturers, using only their assigned prefixes, uniquely assign the three least-significant octets of every Ethernet interface they produce.

## Repeaters and Hubs

A repeater is an electronic device that receives a network signal, cleans it of unnecessary noise and regenerates it. The signal is retransmitted at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. With fiber optics, repeaters can be tens or even hundreds of kilometers apart.

A repeater with multiple ports is known as a hub. Repeaters work on the physical layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay that affects network performance. As a result, many network architectures limit the number of repeaters that can be used in a row, e.g., the Ethernet 5-4-3 rule.

Hubs have been mostly obsoleted by modern switches; but repeaters are used for long distance links, notably undersea cabling.

## Bridges

A network bridge connects and filters traffic between two network segments at the data link layer (layer 2) of the OSI model to form a single network. This breaks the network's collision domain but maintains a unified broadcast domain. Network segmentation breaks down a large, congested network into an aggregation of smaller, more efficient networks.

Bridges come in three basic types:

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

## Switches

A network switch is a device that forwards and filters OSI layer 2 datagrams (frames) between ports based on the destination MAC address in each frame. A switch is distinct from a hub in that it only forwards the frames to the physical ports involved in the communication rather than all ports connected. It can be thought of as a multi-port bridge. It learns to associate physical ports to MAC addresses by examining the source addresses of received frames. If an unknown destination is targeted, the switch broadcasts to all ports but the source. Switches normally have numerous ports, facilitating a star topology for devices, and cascading additional switches.

Multi-layer switches are capable of routing based on layer 3 addressing or additional logical levels. The term *switch* is often used loosely to include devices such as routers

and bridges, as well as devices that may distribute traffic based on load or based on application content (e.g., a Web URL identifier).

## Routers




A typical home or small office router showing the ADSL telephone line and Ethernet network cable connections

A router is an internetworking device that forwards packets between networks by processing the routing information included in the packet or datagram (Internet protocol information from layer 3). The routing information is often processed in conjunction with the routing table (or forwarding table). A router uses its routing table to determine where to forward packets. A destination in a routing table can include a "null" interface, also known as the "black hole" interface because data can go into it, however, no further processing is done for said data, i.e. the packets are dropped.

## Modems

Modems (MOdulator-DEModulator) are used to connect network nodes via wire not originally designed for digital network traffic, or for wireless. To do this one or more carrier signals are modulated by the digital signal to produce an analog signal that can be tailored to give the required properties for transmission. Modems are commonly used for telephone lines, using a Digital Subscriber Line technology.

## Firewalls

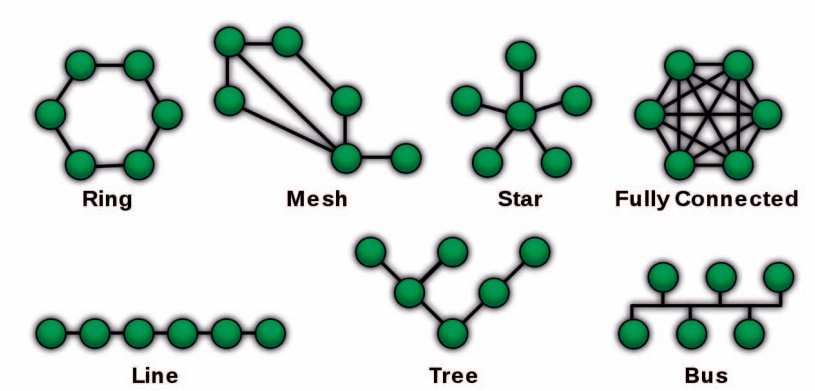
A firewall is a network device for controlling network security and access rules. Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.

## Network Structure

Network topology is the layout or organizational hierarchy of interconnected nodes of a computer network. Different network topologies can affect throughput, but reliability is

often more critical. With many technologies, such as bus networks, a single failure can cause the network to fail entirely. In general the more interconnections there are, the more robust the network is; but the more expensive it is to install.

## Common Layouts



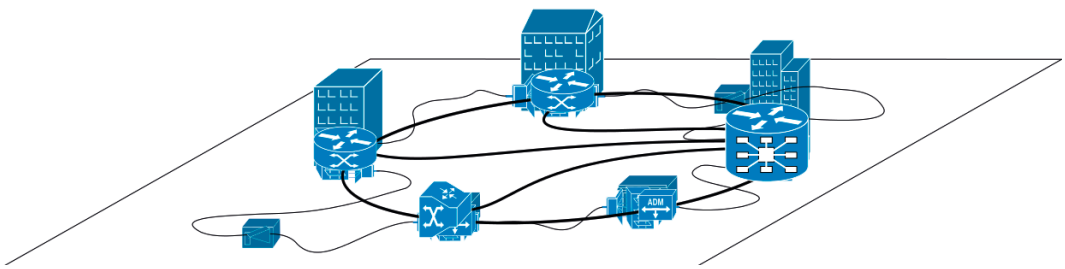

Common network topologies

Common layouts are:

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

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

## *Overlay Network*




A sample overlay network

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay network are connected by virtual or logical links. Each link corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one. For example, many peer-to-peer networks are overlay networks. They are organized as nodes of a virtual system of links that run on top of the Internet.

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

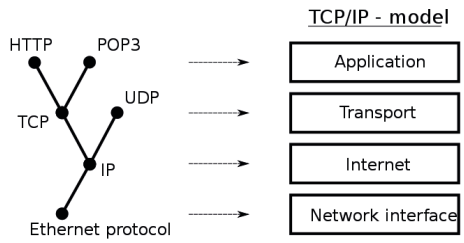
The most striking example of an overlay network is the Internet itself. The Internet itself was initially built as an overlay on the telephone network.Even today, each Internet node can communicate with virtually any other through an underlying mesh of sub-networks of wildly different topologies and technologies. Address resolution and routing are the means that allow mapping of a fully connected IP overlay network to its underlying network.

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

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

For example, Akamai Technologies manages an overlay network that provides reliable, efficient content delivery (a kind of multicast). Academic research includes end system multicast, resilient routing and quality of service studies, among others.

## Communications Protocols




The TCP/IP model or Internet layering scheme and its relation to common protocols often layered on top of it.

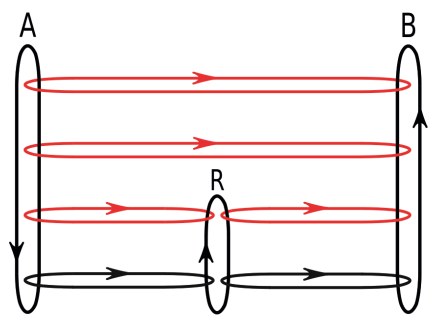



**Figure 4:** Message flows (A-B) in the presence of a router (R), red flows are effective communication paths, black paths are the actual paths.

A communications protocol is a set of rules for exchanging information over network links. In a protocol stack (also see the OSI model), each protocol leverages the services of the protocol below it. An important example of a protocol stack is HTTP (the World Wide Web protocol) running over TCP over IP (the Internet protocols) over IEEE 802.11 (the Wi-Fi protocol). This stack is used between the wireless router and the home user's personal computer when the user is surfing the web.

Whilst the use of protocol layering is today ubiquitous across the field of computer networking, it has been historically criticized by many researchers for two principal reasons. Firstly, abstracting the protocol stack in this way may cause a higher layer to duplicate functionality of a lower layer, a prime example being error recovery on both a per-link basis and an end-to-end basis. Secondly, it is common that a protocol implementation at one layer may require data, state or addressing information that is only present at another layer, thus defeating the point of separating the layers in the first place. For example, TCP uses the ECN field in the IPv4 header as an indication of congestion; IP is a network layer protocol whereas TCP is a transport layer protocol.

Communication protocols have various characteristics. They may be connection-oriented or connectionless, they may use circuit mode or packet switching, and they may use hierarchical addressing or flat addressing.

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

## IEEE 802

IEEE 802 is a family of IEEE standards dealing with local area networks and metropolitan area networks. The complete IEEE 802 protocol suite provides a diverse set of networking capabilities. The protocols have a flat addressing scheme. They operate mostly at levels 1 and 2 of the OSI model.

For example, MAC bridging (IEEE 802.1D) deals with the routing of Ethernet packets using a Spanning Tree Protocol. IEEE 802.1Q describes VLANs, and IEEE 802.1X defines a port-based Network Access Control protocol, which forms the basis for the authentication mechanisms used in VLANs (but it is also found in WLANs) – it is what the home user sees when the user has to enter a "wireless access key".

## Ethernet

Ethernet, sometimes simply called *LAN*, is a family of protocols used in wired LANs, described by a set of standards together called IEEE 802.3 published by the Institute of Electrical and Electronics Engineers.

## Wireless LAN

Wireless LAN, also widely known as WLAN or Wi-fi, is probably the most well-known member of the IEEE 802 protocol family for home users today. It is standarized by IEEE 802.11 and shares many properties

with wired Ethernet.

## Internet Protocol Suite

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

## SONET/SDH

Synchronous optical networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber using lasers. They were originally designed to transport circuit mode communications from a variety of different sources, primarily to support real-time, uncompressed, circuit-switched

voice encoded in PCM (Pulse-Code Modulation) format. However, due to its protocol neutrality and transport-oriented features, SONET/SDH also was the obvious choice for transporting Asynchronous Transfer Mode (ATM) frames.

## Asynchronous Transfer Mode

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

While the role of ATM is diminishing in favor of next-generation networks, it still plays a role in the last mile, which is the connection between an Internet service provider and the home user.

## Geographic Scale

A network can be characterized by its physical capacity or its organizational purpose. Use of the network, including user authorization and access rights, differ accordingly.

## Nanoscale Network

A nanoscale communication network has key components implemented at the nanoscale including message carriers and leverages physical principles that differ from macroscale communication mechanisms. Nanoscale communication extends communication to very small sensors and actuators such as those found in biological systems and also tends to operate in environments that would be too harsh for classical communication.

## Personal Area Network

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

## Local Area Network

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as a home, school, office building, or closely positioned group

of buildings. Each computer or device on the network is a node. Wired LANs are most likely based on Ethernet technology. Newer standards such as ITU-T G.hn also provide a way to create a wired LAN using existing wiring, such as coaxial cables, telephone lines, and power lines.

The defining characteristics of a LAN, in contrast to a wide area network (WAN), include higher data transfer rates, limited geographic range, and lack of reliance on leased lines to provide connectivity. Current Ethernet or other IEEE 802.3 LAN technologies operate at data transfer rates up to 100 Gbit/s, standarized by IEEE in 2010. Currently, 400 Gbit/s Ethernet is being developed.

A LAN can be connected to a WAN using a router.

### *Home Area Network*

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

### *Storage Area Network*

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

### *Campus Area Network*

A campus area network (CAN) is made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling, etc.) are almost entirely owned by the campus tenant / owner (an enterprise, university, government, etc.). For example, a university campus network is likely to link a variety of campus buildings to connect academic colleges or departments, the library, and student residence halls.

### *Backbone Network*

A backbone network is part of a computer network infrastructure that provides a path for the exchange of information between different LANs or sub-networks. A backbone can tie together diverse networks within the same building, across different buildings, or over a wide area.

For example, a large company might implement a backbone network to connect departments that are located around the world. The equipment that ties together the departmental networks constitutes the network backbone. When designing a network backbone, network performance and network congestion are critical factors to take into account. Normally, the backbone network's capacity is greater than that of the individual networks connected to it.

Another example of a backbone network is the Internet backbone, which is the set of wide area networks (WANs) and core routers that tie together all networks connected to the Internet.

## Metropolitan Area Network

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

## Wide Area Network

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

## Enterprise Private Network

An enterprise private network is a network that a single organization builds to interconnect its office locations (e.g., production sites, head offices, remote offices, shops) so they can share computer resources.

## Virtual Private Network

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

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

### *Global Area Network*

A global area network (GAN) is a network used for supporting mobile across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial wireless LANs.

## Organizational Scope

Networks are typically managed by the organizations that own them. Private enterprise networks may use a combination of intranets and extranets. They may also provide network access to the Internet, which has no single owner and permits virtually unlimited global connectivity.

### *Intranet*

An intranet is a set of networks that are under the control of a single administrative entity. The intranet uses the IP protocol and IP-based tools such as web browsers and file transfer applications. The administrative entity limits use of the intranet to its authorized users. Most commonly, an intranet is the internal LAN of an organization. A large intranet typically has at least one web server to provide users with organizational information. An intranet is also anything behind the router on a local area network.

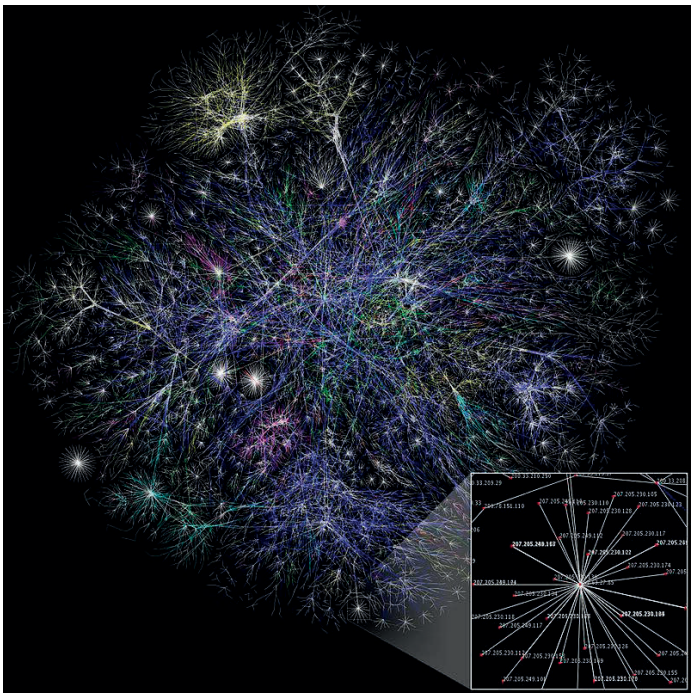
### *Extranet*

An extranet is a network that is also under the administrative control of a single organization, but supports a limited connection to a specific external network. For example, an organization may provide access to some aspects of its intranet to share data with its business partners or customers. These other entities are not necessarily trusted from a security standpoint. Network connection to an extranet is often, but not always, implemented via WAN technology.

### *Internetwork*

An internetwork is the connection of multiple computer networks via a common routing technology using routers.

## Internet



Partial map of the Internet based on the January 15, 2005 data found on opte.org. Each line is drawn between two nodes, representing two IP addresses. The length of the lines are indicative of the delay between those two nodes. This graph represents less than 30% of the Class C networks reachable.

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

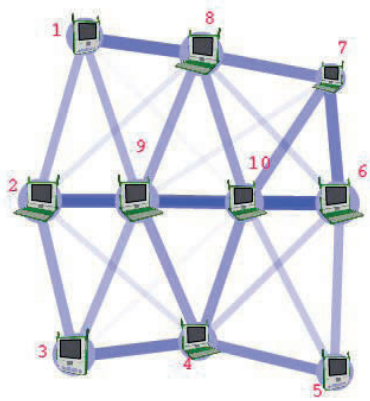
Participants in the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet Protocol Suite and an addressing system (IP addresses) administered by the Internet Assigned Numbers Authority and address registries. Service providers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

## Darknet

A darknet is an overlay network, typically running on the internet, that is only accessible through specialized software. A darknet is an anonymizing network where connections are made only between trusted peers — sometimes called “friends” (F2F) — using non-standard protocols and ports.

Darknets are distinct from other distributed peer-to-peer networks as sharing is anonymous (that is, IP addresses are not publicly shared), and therefore users can communicate with little fear of governmental or corporate interference.

## Routing




Routing calculates good paths through a network for information to take. For example, from node 1 to node 6 the best routes are likely to be 1-8-7-6 or 1-8-10-6, as this has the thickest routes.

Routing is the process of selecting network paths to carry network traffic. Routing is performed for many kinds of networks, including circuit switching networks and packet switched networks.

In packet switched networks, routing directs packet forwarding (the transit of logically addressed network packets from their source toward their ultimate destination) through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. The routing process usually directs forwarding on the basis of routing tables, which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing.

There are usually multiple routes that can be taken, and to choose between them, different elements can be considered to decide which routes get installed into the routing table, such as (sorted by priority):

- *Prefix-Length*: where longer subnet masks are preferred (independent if it is within a routing protocol or over different routing protocol)
- *Metric*: where a lower metric/cost is preferred (only valid within one and the same routing protocol)

- *Administrative distance*: where a lower distance is preferred (only valid between different routing protocols)

Most routing algorithms use only one network path at a time. Multipath routing techniques enable the use of multiple alternative paths.

Routing, in a more narrow sense of the term, is often contrasted with bridging in its assumption that network addresses are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within localized environments.

## Network Service

Network services are applications hosted by servers on a computer network, to provide some functionality for members or users of the network, or to help the network itself to operate.

The World Wide Web, E-mail, printing and network file sharing are examples of well-known network services. Network services such as DNS (Domain Name System) give names for IP and MAC addresses (people remember names like "nm.lan" better than numbers like "210.121.67.18"), and DHCP to ensure that the equipment on the network has a valid IP address.

Services are usually based on a service protocol that defines the format and sequencing of messages between clients and servers of that network service.

## Network Performance

### *Quality of Service*

Depending on the installation requirements, network performance is usually measured by the quality of service of a telecommunications product. The parameters that affect this typically can include throughput, jitter, bit error rate and latency.

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

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

There are many ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modelled instead of measured. For example, state transition diagrams are often used to model queuing performance in a circuit-switched network. The network planner uses these diagrams to analyze how the network performs in each state, ensuring that the network is optimally designed.

### Network Congestion

Network congestion occurs when a link or node is carrying so much data that its quality of service deteriorates. Typical effects include queueing delay, packet loss or the blocking of new connections. A consequence of these latter two is that incremental increases in offered load lead either only to small increase in network throughput, or to an actual reduction in network throughput.

Network protocols that use aggressive retransmissions to compensate for packet loss tend to keep systems in a state of network congestion—even after the initial load is reduced to a level that would not normally induce network congestion. Thus, networks using these protocols can exhibit two stable states under the same level of load. The stable state with low throughput is known as *congestive collapse*.

Modern networks use congestion control and congestion avoidance techniques to try to avoid congestion collapse. These include: exponential backoff in protocols such as 802.11's CSMA/CA and the original Ethernet, window reduction in TCP, and fair queueing in devices such as routers. Another method to avoid the negative effects of network congestion is implementing priority schemes, so that some packets are transmitted with higher priority than others. Priority schemes do not solve network congestion by themselves, but they help to alleviate the effects of congestion for some services. An example of this is 802.1p. A third method to avoid network congestion is the explicit allocation of network resources to specific flows. One example of this is the use of Contention-Free Transmission Opportunities (CFTXOPs) in the ITU-T G.hn standard, which provides high-speed (up to 1 Gbit/s) Local area networking over existing home wires (power lines, phone lines and coaxial cables).

For the Internet RFC 2914 addresses the subject of congestion control in detail.

### Network Resilience

Network resilience is "the ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation."

## Security

### Network Security

Network security consists of provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and its network-accessible resources. Network security is the authorization of

access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network security is used on a variety of computer networks, both public and private, to secure daily transactions and communications among businesses, government agencies and individuals.

## Network Surveillance

Network surveillance is the monitoring of data being transferred over computer networks such as the Internet. The monitoring is often done surreptitiously and may be done by or at the behest of governments, by corporations, criminal organizations, or individuals. It may or may not be legal and may or may not require authorization from a court or other independent agency.

Computer and network surveillance programs are widespread today, and almost all Internet traffic is or could potentially be monitored for clues to illegal activity.

Surveillance is very useful to governments and law enforcement to maintain social control, recognize and monitor threats, and prevent/investigate criminal activity. With the advent of programs such as the Total Information Awareness program, technologies such as high speed surveillance computers and biometrics software, and laws such as the Communications Assistance For Law Enforcement Act, governments now possess an unprecedented ability to monitor the activities of citizens.

However, many civil rights and privacy groups—such as Reporters Without Borders, the Electronic Frontier Foundation, and the American Civil Liberties Union—have expressed concern that increasing surveillance of citizens may lead to a mass surveillance society, with limited political and personal freedoms. Fears such as this have led to numerous lawsuits such as *Hepting v. AT&T*. The hacktivist group Anonymous has hacked into government websites in protest of what it considers "draconian surveillance".

## End to end Encryption

End-to-end encryption (E2EE) is a digital communications paradigm of uninterrupted protection of data traveling between two communicating parties. It involves the originating party encrypting data so only the intended recipient can decrypt it, with no dependency on third parties. End-to-end encryption prevents intermediaries, such as Internet providers or application service providers, from discovering or tampering with communications. End-to-end encryption generally protects both confidentiality and integrity.

Examples of end-to-end encryption include PGP for email, OTR for instant messaging, ZRTP for telephony, and TETRA for radio.

Typical server-based communications systems do not include end-to-end encryption. These systems can only guarantee protection of communications between clients and servers, not between the communicating parties themselves. Examples of non-E2EE systems are Google Talk, Yahoo Messenger, Facebook, and Dropbox. Some such systems, for example LavaBit and SecretInk, have even described themselves as offering "end-to-end" encryption when they do not. Some systems that normally offer end-to-end encryption

have turned out to contain a back door that subverts negotiation of the encryption key between the communicating parties, for example Skype or Hushmail.

The end-to-end encryption paradigm does not directly address risks at the communications endpoints themselves, such as the technical exploitation of clients, poor quality random number generators, or key escrow. E2EE also does not address traffic analysis, which relates to things such as the identities of the end points and the times and quantities of messages that are sent.

## Views of Networks

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

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

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

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

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

## REFERENCES


1. Computer network definition, retrieved 2011-11-12
2. “История о том, как пионер кибернетики оказался не нужен СССР” [The story of how a cybernetics pioneer became unnecessary to the USSR]. ria.ru (in Russian). МИА «Россия сегодня». 2010-08-09. Retrieved 2015-03-04. Главным делом жизни Китова, увы, не доведенным до практического воплощения, можно считать разработку плана создания компьютерной сети (Единой государственной сети вычислительных центров - ЕГСВЦ) для управления народным хозяйством и одновременно для решения военных задач. Этот план Анатолий Иванович предложил сразу в высшую инстанцию, направив в январе 1959 года письмо генсеку КПСС Никите Хрущеву. Не получив ответа (хотя начинание на словах было поддержано в различных кругах), осенью того же года он заново направляет на самый верх письмо, приложив к нему 200-страничный детальный проект, получивший название ‹Красной книги›. [One can regard the magnum opus of Kitov’s career as his elaboration of the plan – unfortunately never brought into practical form – for the establishment of a computer network (the Unified State Network of Computer Centres – EGSVTs) for the control of the national economy and simultaneously for the resolution of military tasks. Anatolii Ivanovich presented this plan directly to the highest levels, sending a letter in January 1959 to the General Secretary of the Communist Party of the Soviet Union Nikita Khrushchev. Not receiving a reply (although supported in various circles), in the autumn of the same year he again sent a letter to the very top, appending a 200-page detailed project plan, called the ‹Red Book’]
3. Chris Sutton. “Internet Began 35 Years Ago at UCLA with First Message Ever Sent Between Two Computers”. UCLA. Archived from the original on March 8, 2008.
4. Ethernet: Distributed Packet Switching for Local Computer Networks, Robert M. Metcalfe and David R. Boggs, Communications of the ACM (pp 395–404, Vol. 19, No. 5), July 1976.
5. Spurgeon, Charles E. (2000). Ethernet The Definitive Guide. O’Reilly & Associates. ISBN 1-56592-660-9.
6. , The Disadvantages of Wired Technology, Laura Acevedo, Demand Media.
7. “Bergen Linux User Group’s CPIP Implementation”. Blug.linux.no. Retrieved 2014-03-01.
8. A. Hooke (September 2000), Interplanetary Internet (PDF), Third Annual International Symposium on Advanced Radio Technologies, archived from the original (PDF) on 2012-01-13, retrieved 2011-11-12
9. “Define switch.”. WWW.Wikipedia.com. Retrieved April 8, 2008.
10. http://compnetworking.about.com/cs/internetworking/g/bldef_bridge.htm
11. D. Andersen; H. Balakrishnan; M. Kaashoek; R. Morris (October 2001), Resilient Overlay Networks, Association for Computing Machinery, retrieved 2011-11-12

12. "End System Multicast". project web site. Carnegie Mellon University. Retrieved May 25, 2013.
13. Wakeman, I (Jan 1992). "Layering considered harmful". IEEE Network: 20–24.
14. Kurose, James; Ross, Kieth (2005). Computer Networking: A Top-Down Approach. Pearson.
15. For an interesting write-up of the technologies involved, including the deep stacking of communications protocols used, see.Martin, Thomas. "Design Principles for DSL-Based Access Solutions" (PDF). Retrieved 18 June 2011.
16. Nanoscale Communication Networks, Bush, S. F., ISBN 978-1-60807-003-9, Artech House, 2010.
17. "personal area network (PAN)". Retrieved January 29, 2011.
18. New global standard for fully networked home, ITU-T, 2008-12-12, retrieved 2011-11-12
19. IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force, retrieved 2011-11-12
20. "Mobile Broadband Wireless connections (MBWA)". Retrieved 2011-11-12.
21. Mansfield-Devine, Steve (December 2009). "Darknets". Computer Fraud & Security. 2009 (12): 4–6. doi:10.1016/S1361-3723(09)70150-2.
22. Wood, Jessica (2010). "The Darknet: A Digital Copyright Revolution" (PDF). Richmond Journal of Law and Technology. 16 (4). Retrieved 25 October 2011.
23. rfc5321
24. RFC 1035, Domain names – Implementation and Specification, P. Mockapetris (November 1987)
25. Peterson LL, Davie BS. (2011). Computer Networks: A Systems Approach.
26. Teletraffic Engineering Handbook (PDF), ITU-T Study Group 2, archived from the original (PDF) on 2007-01-11
27. Telecommunications Magazine Online, Americas January 2003, Issue Highlights, Online Exclusive: Broadband Access Maximum Performance, Retrieved on February 13, 2005.
28. "State Transition Diagrams". Retrieved July 13, 2003.
29. "Definitions: Resilience". ResiliNets Research Initiative. Retrieved 2011-11-12.
30. Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attack". Lecture Notes in Computer Science. Lecture Notes in Computer Science. 3285: 317–323. doi:10.1007/978-3-540-30176-9_41. ISBN 978-3-540-23659-7.
31. "Is the U.S. Turning Into a Surveillance Society?". American Civil Liberties Union. Retrieved March 13, 2009.
32. "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society" (PDF). American Civil Liberties Union. January 15, 2003. Retrieved March 13, 2009.

33. "Anonymous hacks UK government sites over ‹draconian surveillance' ", Emil Protalinski, ZDNet, 7 April 2012, retrieved 12 March 2013
34. Hacktivists in the frontline battle for the internet retrieved 17 June 2012

CHAPTER 2

# History of the Internet

## Chapter Contents

- **Introduction**

The Internet has always been an emerging technology and an emerging ideal. What follows is a selective and developing chronology of some of the most important events in the cultural and technological development of cyberspace and the internet. Primarily intended for interested readers without a technological background, this selective chronology seeks to present a brief narrative chronology of the technological innovation of the internet and its predecessors as well as accompanying consumer and cultural developments.

## INTRODUCTION

The history of the Internet begins with the development of electronic computers in the 1950s. Initial concepts of packet networking originated in several computer science laboratories in the United States, United Kingdom, and France. The US Department of Defense awarded contracts as early as the 1960s for packet network systems, including the development of the ARPANET. The first message was sent over the ARPANET from computer science Professor Leonard Kleinrock's laboratory at University of California, Los Angeles (UCLA) to the second network node at Stanford Research Institute (SRI).

Packet switching networks such as ARPANET, NPL network, CYCLADES, Merit Network, Tymnet, and Telenet, were developed in the late 1960s and early 1970s using a variety of communications protocols. Donald Davies first designed a packet-switched

network at the National Physics Laboratory in the UK, which became a test bed for UK research for almost two decades. The ARPANET project led to the development of protocols for internetworking, in which multiple separate networks could be joined into a network of networks.

Access to the ARPANET was expanded in 1981 when the National Science Foundation (NSF) funded the Computer Science Network (CSNET). In 1982, the Internet protocol suite (TCP/IP) was introduced as the standard networking protocol on the ARPANET. In the early 1980s the NSF funded the establishment for national supercomputing centers at several universities, and provided interconnectivity in 1986 with the NSFNET project, which also created network access to the supercomputer sites in the United States from research and education organizations. Commercial Internet service providers (ISPs) began to emerge in the very late 1980s. The ARPANET was decommissioned in 1990. Limited private connections to parts of the Internet by officially commercial entities emerged in several American cities by late 1989 and 1990, and the NSFNET was decommissioned in 1995, removing the last restrictions on the use of the Internet to carry commercial traffic.

In the 1980s, research at CERN in Switzerland by British computer scientist Tim Berners-Lee resulted in the World Wide Web, linking hypertext documents into an information system, accessible from any node on the network. Since the mid-1990s, the Internet has had a revolutionary impact on culture, commerce, and technology, including the rise of near-instant communication by electronic mail, instant messaging, voice over Internet Protocol (VoIP) telephone calls, two-way interactive video calls, and the World Wide Web with its discussion forums, blogs, social networking, and online shopping sites. The research and education community continues to develop and use advanced networks such as NSF's very high speed Backbone Network Service (vBNS), Internet2, and National LambdaRail. Increasing amounts of data are transmitted at higher and higher speeds over fiber optic networks operating at 1-Gbit/s, 10-Gbit/s, or more. The Internet's takeover of the global communication landscape was almost instant in historical terms: it only communicated 1% of the information flowing through two-way telecommunications networks in the year 1993, already 51% by 2000, and more than 97% of the telecommunicated information by 2007. Today the Internet continues to grow, driven by ever greater amounts of online information, commerce, entertainment, and social networking.

## Precursors

The concept of data communication – transmitting data between two different places through an electromagnetic medium such as radio or an electric wire – predates the introduction of the first computers. Such communication systems were typically limited to point to point communication between two end devices. Telegraph systems and telex machines can be considered early precursors of this kind of communication. The Telegraph in the late 19th century was the first fully digital communication system.

Fundamental theoretical work in data transmission and information theory was developed by Claude Shannon, Harry Nyquist, and Ralph Hartley in the early 20th century.

Early computers had a central processing unit and remote terminals. As the technology evolved, new systems were devised to allow communication over longer distances (for

terminals) or with higher speed (for interconnection of local devices) that were necessary for the mainframe computer model. These technologies made it possible to exchange data (such as files) between remote computers. However, the point-to-point communication model was limited, as it did not allow for direct communication between any two arbitrary systems; a physical link was necessary. The technology was also considered unsafe for strategic and military use because there were no alternative paths for the communication in case of an enemy attack.

## Development of Wide-Area Networking

With limited exceptions, the earliest computers were connected directly to terminals used by individual users, typically in the same building or site. Such networks became known as local-area networks (LANs). Networking beyond this scope, known as wide-area networks (WANs), emerged during the 1950s and became established during the 1960s.

### *Inspiration*

J. C. R. Licklider, Vice President at Bolt Beranek and Newman, Inc., proposed a global network in his January 1960 paper *Man-Computer Symbiosis*:

A network of such [computers], connected to one another by wide-band communication lines [which provided] the functions of present-day libraries together with anticipated advances in information storage and retrieval and [other] symbiotic functions

In August 1962, Licklider and Welden Clark published the paper "On-Line Man-Computer Communication"which was one of the first descriptions of a networked future.

In October 1962, Licklider was hired by Jack Ruina as director of the newly established Information Processing Techniques Office (IPTO) within DARPA, with a mandate to interconnect the United States Department of Defense's main computers at Cheyenne Mountain, the Pentagon, and SAC HQ. There he formed an informal group within DARPA to further computer research. He began by writing memos describing a distributed network to the IPTO staff, whom he called "Members and Affiliates of the Intergalactic Computer Network". As part of the information processing office's role, three network terminals had been installed: one for System Development Corporation in Santa Monica, one for Project Genie at University of California, Berkeley, and one for the Compatible Time-Sharing System project at Massachusetts Institute of Technology (MIT). Licklider's identified need for inter-networking would become obvious by the apparent waste of resources this caused.

For each of these three terminals, I had three different sets of user commands. So if I was talking online with someone at S.D.C. and I wanted to talk to someone I knew at Berkeley or M.I.T. about this, I had to get up from the S.D.C. terminal, go over and log into the other terminal and get in touch with them.... I said, oh man, it's obvious what to do: If you have these three terminals, there ought to be one terminal that goes anywhere you want to go where you have interactive computing. That idea is the ARPAnet.

Although he left the IPTO in 1964, five years before the ARPANET went live, it was his vision of universal networking that provided the impetus for his successors such

as Lawrence Roberts and Robert Taylor to further the ARPANET development. Licklider later returned to lead the IPTO in 1973 for two years.

### *Development of Packet Switching*

The issue of connecting separate physical networks to form one logical network was the first of many problems. In the 1960s, Paul Baran of the RAND Corporation produced a study of survivable networks for the U.S. military in the event of nuclear war. Information transmitted across Baran's network would be divided into what he called "message-blocks". Independently, Donald Davies (National Physical Laboratory, UK), proposed and was the first to put into practice a similar network based on what he called packet-switching, the term that would ultimately be adopted. Leonard Kleinrock (MIT) developed a mathematical theory behind this technology (without the packets). Packet-switching provides better bandwidth utilization and response times than the traditional circuit-switching technology used for telephony, particularly on resource-limited interconnection links.

Packet switching is a rapid store and forward networking design that divides messages up into arbitrary packets, with routing decisions made per-packet. Early networks used message switched systems that required rigid routing structures prone to single point of failure. This led Tommy Krash and Paul Baran's U.S. military-funded research to focus on using message-blocks to include network redundancy.

## Networks that Led to the Internet

### *Arpanet*

Promoted to the head of the information processing office at Defense Advanced Research Projects Agency (DARPA), Robert Taylor intended to realize Licklider's ideas of an interconnected networking system. Bringing in Larry Roberts from MIT, he initiated a project to build such a network. The first ARPANET link was established between the University of California, Los Angeles (UCLA) and the Stanford Research Institute at 22:30 hours on October 29, 1969.

"We set up a telephone connection between us and the guys at SRI ...", Kleinrock ... said in an interview: "We typed the L and we asked on the phone,

"Do you see the L?"

"Yes, we see the L," came the response.

We typed the O, and we asked, "Do you see the O."

"Yes, we see the O."

Then we typed the G, and the system crashed ...

Yet a revolution had begun" ....




35 Years of the Internet, 1969–2004. Stamp of Azerbaijan, 2004.

By December 5, 1969, a 4-node network was connected by adding the University of Utah and the University of California, Santa Barbara. Building on ideas developed in ALOHAnet, the ARPANET grew rapidly. By 1981, the number of hosts had grown to 213, with a new host being added approximately every twenty days.

ARPANET development was centered around the Request for Comments (RFC) process, still used today for proposing and distributing Internet Protocols and Systems. RFC 1, entitled "Host Software", was written by Steve Crocker from the University of California, Los Angeles, and published on April 7, 1969. These early years were documented in the 1972 film Computer Networks: The Heralds of Resource Sharing.

ARPANET became the technical core of what would become the Internet, and a primary tool in developing the technologies used. The early ARPANET used the Network Control Program (NCP, sometimes Network Control Protocol) rather than TCP/IP. On January 1, 1983, known as flag day, NCP on the ARPANET was replaced by the more flexible and powerful family of TCP/IP protocols, marking the start of the modern Internet.

International collaborations on ARPANET were sparse. For various political reasons, European developers were concerned with developing the X.25 networks. Notable exceptions were the *Norwegian Seismic Array* (NORSAR) in 1972, followed in 1973 by Sweden with satellite links to the Tanum Earth Station and Peter Kirstein's research group in the UK, initially at the Institute of Computer Science, London University and later at University College London.

## NPL

In 1965, Donald Davies of the National Physical Laboratory (United Kingdom) proposed a national data network based on packet-switching. The proposal was not taken up nationally, but by 1970 he had designed and built the Mark I packet-switched network to meet the needs of the multidisciplinary laboratory and prove the technology under operational conditions. By 1976 12 computers and 75 terminal devices were attached and more were added until the network was replaced in 1986. NPL, followed by ARPANET, were the first two networks in the world to use packet switching.

### *Merit Network*

The Merit Network was formed in 1966 as the Michigan Educational Research Information Triad to explore computer networking between three of Michigan's public universities as a means to help the state's educational and economic development. With initial support from the State of Michigan and the National Science Foundation (NSF), the packet-switched network was first demonstrated in December 1971 when an interactive host to host connection was made between the IBM mainframe computer systems at the University of Michigan in Ann Arbor and Wayne State University in Detroit. In October 1972 connections to the CDC mainframe at Michigan State University in East Lansing completed the triad. Over the next several years in addition to host to host interactive connections the network was enhanced to support terminal to host connections, host to host batch connections (remote job submission, remote printing, batch file transfer), interactive file transfer, gateways to the Tymnet and Telenetpublic data networks, X.25 host attachments, gateways to X.25 data networks, Ethernet attached hosts, and eventually TCP/IP and additional public universities in Michigan join the network. All of this set the stage for Merit's role in the NSFNET project starting in the mid-1980s.

## Cyclades

The CYCLADES packet switching network was a French research network designed and directed by Louis Pouzin. First demonstrated in 1973, it was developed to explore alternatives to the initial ARPANET design and to support network research generally. It was the first network to make the hosts responsible for the reliable delivery of data, rather than the network itself, using unreliable datagrams and associated end-to-end protocol mechanisms.

### *X.25 and Public Data Networks*



1974 ABC interview with Arthur C. Clarke, in which he describes a future of ubiquitous networked personal computers.

Based on ARPA's research, packet switching network standards were developed by the International Telecommunication Union (ITU) in the form of X.25 and related standards. While using packet switching, X.25 is built on the concept of virtual circuits emulating traditional telephone connections. In 1974, X.25 formed the basis for the SERCnet network between British academic and research sites, which later became JANET. The initial ITU Standard on X.25 was approved in March 1976.

The British Post Office, Western Union International and Tymnet collaborated to create the first international packet switched network, referred to as the International Packet Switched Service (IPSS), in 1978. This network grew from Europe and the US to cover Canada, Hong Kong, and Australia by 1981. By the 1990s it provided a worldwide networking infrastructure.

Unlike ARPANET, X.25 was commonly available for business use. Telenet offered its Telemail electronic mail service, which was also targeted to enterprise use rather than the general email system of the ARPANET.

The first public dial-in networks used asynchronous TTY terminal protocols to reach a concentrator operated in the public network. Some networks, such as CompuServe, used X.25 to multiplex the terminal sessions into their packet-switched backbones, while others, such as Tymnet, used proprietary protocols. In 1979, CompuServe became the first service to offer electronic mail capabilities and technical support to personal computer users. The company broke new ground again in 1980 as the first to offer real-time chat with its CB Simulator. Other major dial-in networks were America Online (AOL) and Prodigy that also provided communications, content, and entertainment features. Many bulletin board system (BBS) networks also provided on-line access, such as FidoNet which was popular amongst hobbyist computer users, many of them hackers and amateur radio operators.

## *UUCP and Usenet*

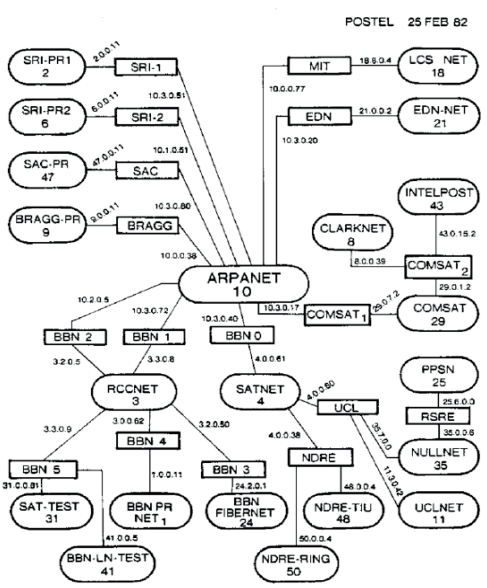
In 1979, two students at Duke University, Tom Truscott and Jim Ellis, originated the idea of using Bourne shell scripts to transfer news and messages on a serial line UUCP connection with nearby University of North Carolina at Chapel Hill. Following public release of the software in 1980, the mesh of UUCP hosts forwarding on the Usenet news rapidly expanded. UUCPnet, as it would later be named, also created gateways and links between FidoNet and dial-up BBS hosts. UUCP networks spread quickly due to the lower costs involved, ability to use existing leased lines, X.25 links or even ARPANET connections, and the lack of strict use policies compared to later networks like CSNET and Bitnet. All connects were local. By 1981 the number of UUCP hosts had grown to 550, nearly doubling to 940 in 1984. – Sublink Network, operating since 1987 and officially founded in Italy in 1989, based its interconnectivity upon UUCP to redistribute mail and news groups messages throughout its Italian nodes (about 100 at the time) owned both by private individuals and small companies. Sublink Network represented possibly one of the first examples of the Internet technology becoming progress through popular diffusion.

## *Merging the Networks and Creating the Internet (1973–95)*



A Stanford Research Institute's Packet Radio Van, site of the first three-way internetworked transmission.

## *TCP/IP*




Map of the TCP/IP test network in February 1982

With so many different network methods, something was needed to unify them. Robert E. Kahn of DARPA and ARPANET recruited Vinton Cerf of Stanford University to work with him on the problem. By 1973, they had worked out a fundamental reformulation, where the differences between network protocols were hidden by using a common internetwork protocol, and instead of the network being responsible for reliability, as in the ARPANET, the hosts became responsible. Cerf credits Hubert Zimmermann, Gerard LeLann and Louis Pouzin (designer of the CYCLADES network) with important work on this design.

The specification of the resulting protocol, *RFC 675 – Specification of Internet Transmission Control Program*, by Vinton Cerf, Yogen Dalal and Carl Sunshine, Network Working Group, December 1974, contains the first attested use of the term *internet*, as a shorthand for *internetworking*; later RFCs repeat this use, so the word started out as an adjective rather than the noun it is today.

With the role of the network reduced to the bare minimum, it became possible to join almost any networks together, no matter what their characteristics were, thereby solving Kahn's initial problem. DARPA agreed to fund development of prototype software, and after several years of work, the first demonstration of a gateway between the Packet Radio network in the SF Bay area and the ARPANET was conducted by the Stanford Research Institute. On November 22, 1977 a three network demonstration was conducted including the ARPANET, the SRI's Packet Radio Van on the Packet Radio Network and the Atlantic Packet Satellite network.

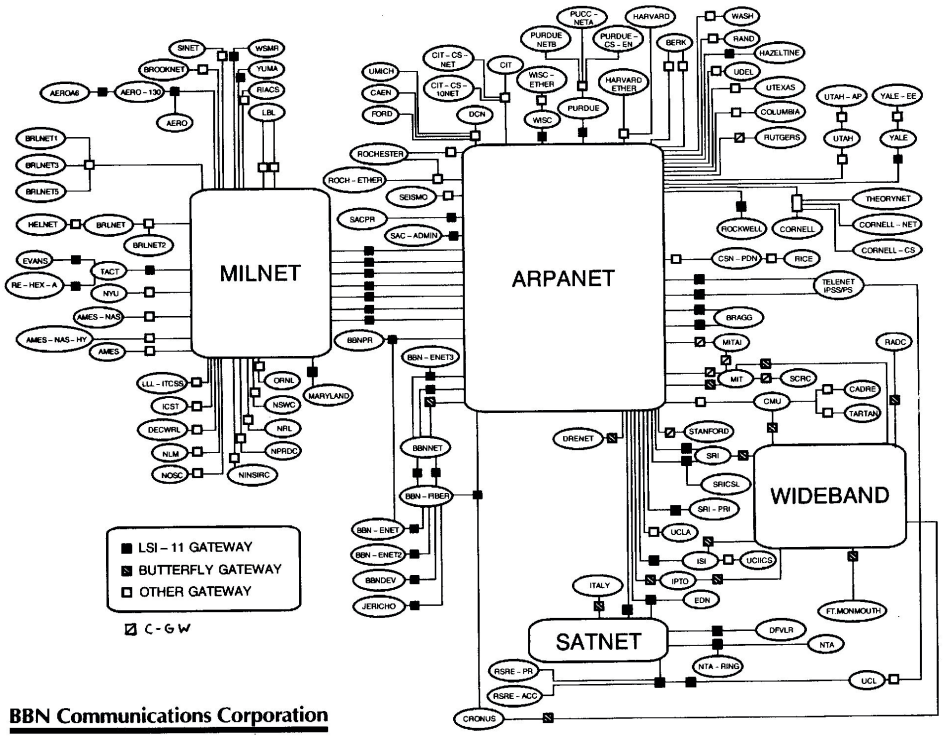
Stemming from the first specifications of TCP in 1974, TCP/IP emerged in mid-late 1978 in nearly its final form, as used for the first decades of the Internet, known as "IPv4". (IPv4 eventually became superseded by its successor, called "IPv6", but this was largely due to the sheer number of devices being connected post-2005, which overwhelmed the numbers that IPv4 had been able to accommodate worldwide. However, due to IPv4's entrenched position by that time, the shift is still in its early stages as of 2015, and expected to take many years, decades, or perhaps longer, to complete).

The associated standards for IPv4 were published by 1981 as RFCs 791, 792 and 793, and adopted for use. DARPA sponsored or encouraged the development of TCP/IP implementations for many operating systems and then scheduled a migration of all hosts on all of its packet networks to TCP/IP. On January 1, 1983, known as flag day, TCP/IP protocols became the only approved protocol on the ARPANET, replacing the earlier NCP protocol.

## From ARPANET to NSFNET

After the ARPANET had been up and running for several years, ARPA looked for another agency to hand off the network to; ARPA's primary mission was funding cutting edge research and development, not running a communications utility. Eventually, in July 1975, the network had been turned over to the Defense Communications Agency, also part of the Department of Defense. In 1983, the U.S. military portion of the ARPANET was broken off as a separate network, the MILNET. MILNET subsequently became the unclassified but military-only NIPRNET, in parallel with the SECRET-level SIPRNET and

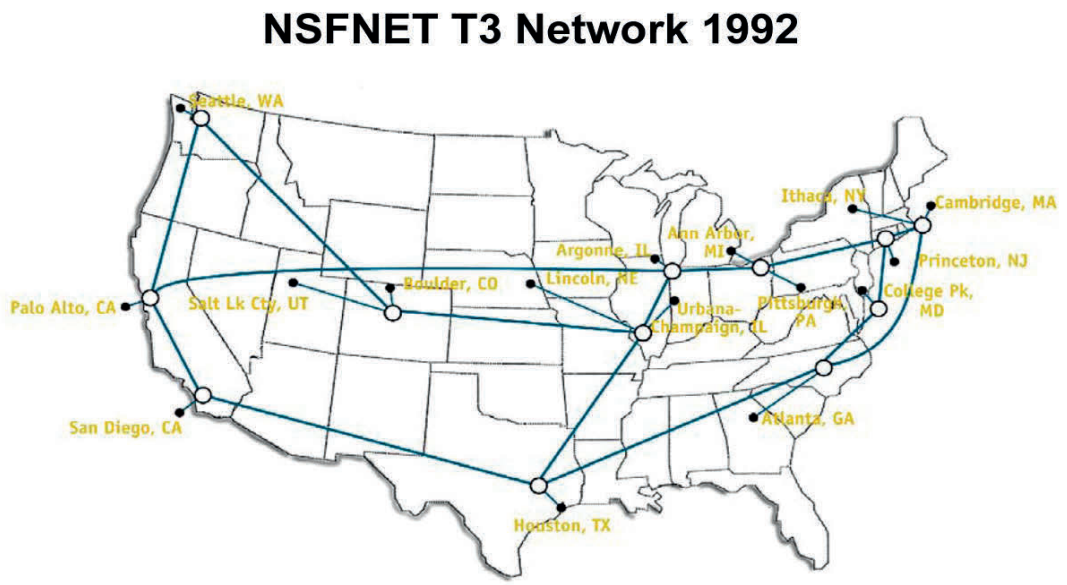
JWICS for TOP SECRET and above. NIPRNET does have controlled security gateways to the public Internet.




BBN Technologies TCP/IP Internet map of early 1986.

The networks based on the ARPANET were government funded and therefore restricted to noncommercial uses such as research; unrelated commercial use was strictly forbidden. This initially restricted connections to military sites and universities. During the 1980s, the connections expanded to more educational institutions, and even to a growing number of companies such as Digital Equipment Corporation and Hewlett-Packard, which were participating in research projects or providing services to those who were.

Several other branches of the U.S. government, the National Aeronautics and Space Administration (NASA), the National Science Foundation (NSF), and the Department of Energy (DOE) became heavily involved in Internet research and started development of a successor to ARPANET. In the mid-1980s, all three of these branches developed the first Wide Area Networks based on TCP/IP. NASA developed the NASA Science Network, NSF developed CSNET and DOE evolved the Energy Sciences Network or ESNet.




T3 NSFNET Backbone, c. 1992

NASA developed the TCP/IP based NASA Science Network (NSN) in the mid-1980s, connecting space scientists to data and information stored anywhere in the world. In 1989, the DECnet-based Space Physics Analysis Network (SPAN) and the TCP/IP-based NASA Science Network (NSN) were brought together at NASA Ames Research Center creating the first multiprotocol wide area network called the NASA Science Internet, or NSI. NSI was established to provide a totally integrated communications infrastructure to the NASA scientific community for the advancement of earth, space and life sciences. As a high-speed, multiprotocol, international network, NSI provided connectivity to over 20,000 scientists across all seven continents.

In 1981 NSF supported the development of the Computer Science Network (CSNET). CSNET connected with ARPANET using TCP/IP, and ran TCP/IP over X.25, but it also supported departments without sophisticated network connections, using automated dial-up mail exchange.

In 1986, the NSF created NSFNET, a 56 kbit/s backbone to support the NSF-sponsored supercomputing centers. The NSFNET also provided support for the creation of regional research and education networks in the United States, and for the connection of university and college campus networks to the regional networks. The use of NSFNET and the regional networks was not limited to supercomputer users and the 56 kbit/s network quickly became overloaded. NSFNET was upgraded to 1.5 Mbit/s in 1988 under a cooperative agreement with the Merit Network in partnership with IBM, MCI, and the State of Michigan. The existence of NSFNET and the creation of Federal Internet Exchanges (FIXes) allowed the ARPANET to be decommissioned in 1990. NSFNET was expanded and upgraded to 45 Mbit/s in 1991, and was decommissioned in 1995 when it was replaced by backbones operated by several commercial Internet Service Providers.

### *Transition Towards the Internet*

The term "internet" was adopted in the first RFC published on the TCP protocol (RFC 675: Internet Transmission Control Program, December 1974) as an abbreviation of the term *internetworking* and the two terms were used interchangeably. In general, an internet was any network using TCP/IP. It was around the time when ARPANET was interlinked with NSFNET in the late 1980s, that the term was used as the name of the network, Internet, being the large and global TCP/IP network.

As interest in networking grew and new applications for it were developed, the Internet's technologies spread throughout the rest of the world. The network-agnostic approach in TCP/IP meant that it was easy to use any existing network infrastructure, such as the IPSS X.25 network, to carry Internet traffic. In 1984, University College London replaced its transatlantic satellite links with TCP/IP over IPSS.

Many sites unable to link directly to the Internet created simple gateways for the transfer of electronic mail, the most important application of the time. Sites with only intermittent connections used UUCP or FidoNet and relied on the gateways between these networks and the Internet. Some gateway services went beyond simple mail peering, such as allowing access to File Transfer Protocol (FTP) sites via UUCP or mail.

Finally, routing technologies were developed for the Internet to remove the remaining centralized routing aspects. The Exterior Gateway Protocol (EGP) was replaced by a new protocol, the Border Gateway Protocol (BGP). This provided a meshed topology for the Internet and reduced the centric architecture which ARPANET had emphasized. In 1994, Classless Inter-Domain Routing (CIDR) was introduced to support better conservation of address space which allowed use of route aggregation to decrease the size of routing tables.

## TCP/IP Goes Global (1980s)

### *Cern, the European Internet, the Link to the Pacific and Beyond*

Between 1984 and 1988 CERN began installation and operation of TCP/IP to interconnect its major internal computer systems, workstations, PCs and an accelerator control system. CERN continued to operate a limited self-developed system (CERNET) internally and several incompatible (typically proprietary) network protocols externally. There was considerable resistance in Europe towards more widespread use of TCP/IP, and the CERN TCP/IP intranets remained isolated from the Internet until 1989.

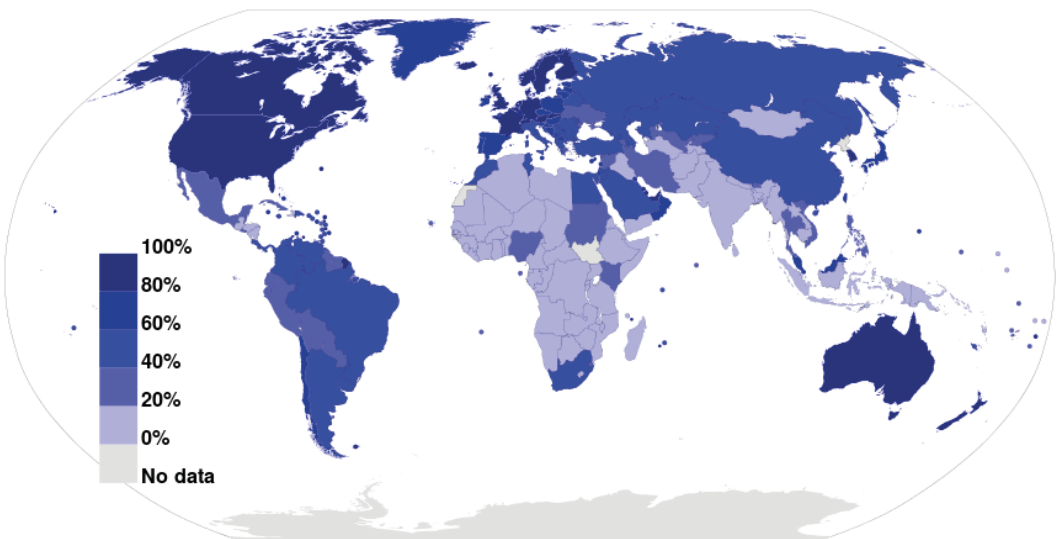
In 1988, Daniel Karrenberg, from Centrum Wiskunde & Informatica (CWI) in Amsterdam, visited Ben Segal, CERN's TCP/IP Coordinator, looking for advice about the transition of the European side of the UUCP Usenet network (much of which ran over X.25 links) over to TCP/IP. In 1987, Ben Segal had met with Len Bosack from the then

still small company Cisco about purchasing some TCP/IP routers for CERN, and was able to give Karrenberg advice and forward him on to Cisco for the appropriate hardware. This expanded the European portion of the Internet across the existing UUCP networks, and in 1989 CERN opened its first external TCP/IP connections. This coincided with the creation of Réseaux IP Européens (RIPE), initially a group of IP network administrators who met regularly to carry out coordination work together. Later, in 1992, RIPE was formally registered as a cooperative in Amsterdam.

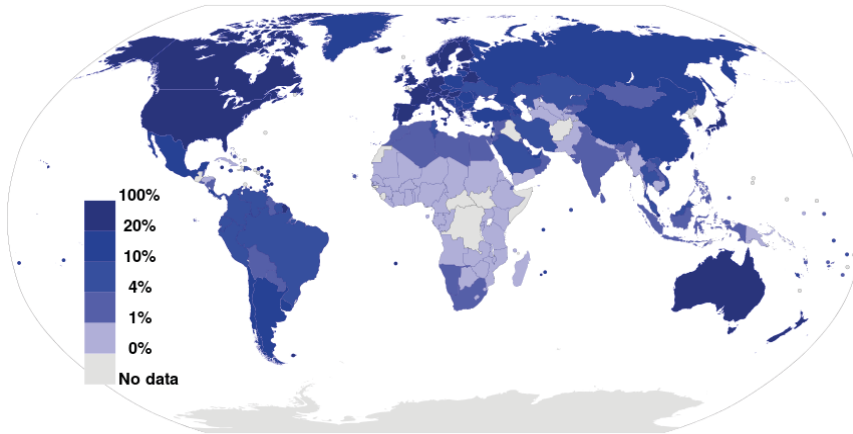
At the same time as the rise of internetworking in Europe, ad hoc networking to ARPA and in-between Australian universities formed, based on various technologies such as X.25 and UUCPNet. These were limited in their connection to the global networks, due to the cost of making individual international UUCP dial-up or X.25 connections. In 1989, Australian universities joined the push towards using IP protocols to unify their networking infrastructures. AARNet was formed in 1989 by the Australian Vice-Chancellors' Committee and provided a dedicated IP based network for Australia.

The Internet began to penetrate Asia in the 1980s. In May 1982 South Korea became the second country to successfully set up TCP/IP IPv4 network. Japan, which had built the UUCP-based network JUNET in 1984, connected to NSFNET in 1989. It hosted the annual meeting of the Internet Society, INET'92, in Kobe. Singapore developed TECHNET in 1990, and Thailand gained a global Internet connection between Chulalongkorn University and UUNET in 1992.

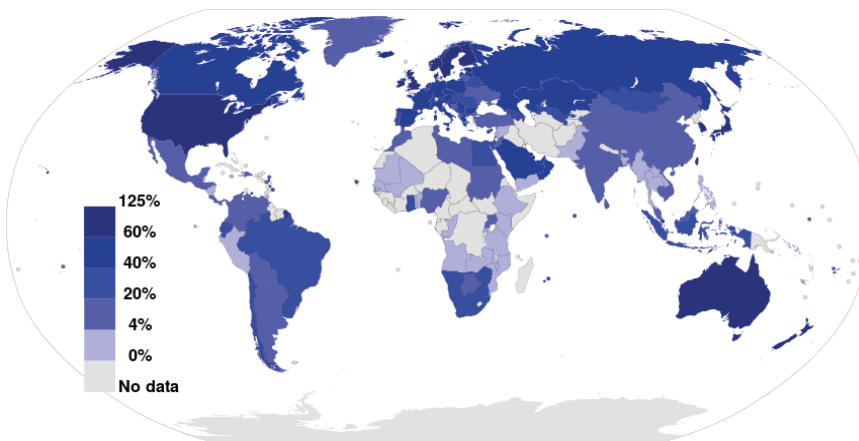
## *The Early Global "Digital Divide" Emerges*




Internet users in 2012 as a percentage of a country's population




Fixed broadband Internet subscriptions in 2012 as a percentage of a country's population




Mobile broadband Internet subscriptions in 2012 as a percentage of a country's population

While developed countries with technological infrastructures were joining the Internet, developing countries began to experience a digital divide separating them from the Internet. On an essentially continental basis, they are building organizations for Internet resource administration and sharing operational experience, as more and more transmission facilities go into place.

## *Africa*

At the beginning of the 1990s, African countries relied upon X.25 IPSS and 2400 baud modem UUCP links for international and internetwork computer communications.

In August 1995, InfoMail Uganda, Ltd., a privately held firm in Kampala now known as InfoCom, and NSN Network Services of Avon, Colorado, sold in 1997 and now known

as Clear Channel Satellite, established Africa's first native TCP/IP high-speed satellite Internet services. The data connection was originally carried by a C-Band RSCC Russian satellite which connected InfoMail's Kampala offices directly to NSN's MAE-West point of presence using a private network from NSN's leased ground station in New Jersey. InfoCom's first satellite connection was just 64 kbit/s, serving a Sun host computer and twelve US Robotics dial-up modems.

In 1996, a USAID funded project, the Leland Initiative, started work on developing full Internet connectivity for the continent. Guinea, Mozambique, Madagascar and Rwanda gained satellite earth stations in 1997, followed by Ivory Coast and Benin in 1998.

Africa is building an Internet infrastructure. AfriNIC, headquartered in Mauritius, manages IP address allocation for the continent. As do the other Internet regions, there is an operational forum, the Internet Community of Operational Networking Specialists.

There are many programs to provide high-performance transmission plant, and the western and southern coasts have undersea optical cable. High-speed cables join North Africa and the Horn of Africa to intercontinental cable systems. Undersea cable development is slower for East Africa; the original joint effort between New Partnership for Africa's Development (NEPAD) and the East Africa Submarine System (Eassy) has broken off and may become two efforts.

### Asia and Oceania

The Asia Pacific Network Information Centre (APNIC), headquartered in Australia, manages IP address allocation for the continent. APNIC sponsors an operational forum, the Asia-Pacific Regional Internet Conference on Operational Technologies (APRICOT).

In 1991, the People's Republic of China saw its first TCP/IP college network, Tsinghua University's TUNET. The PRC went on to make its first global Internet connection in 1994, between the Beijing Electro-Spectrometer Collaboration and Stanford University's Linear Accelerator Center. However, China went on to implement its own digital divide by implementing a country-wide content filter.

### Latin America

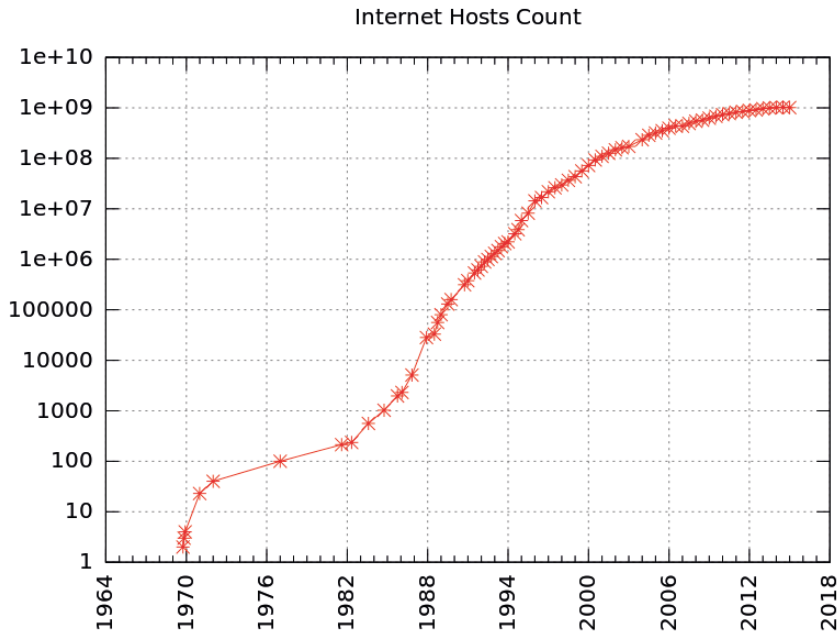
As with the other regions, the Latin American and Caribbean Internet Addresses Registry (LACNIC) manages the IP address space and other resources for its area. LACNIC, headquartered in Uruguay, operates DNS root, reverse DNS, and other key services.

## Rise of the Global Internet (Late 1980s/Early 1990s Onward)

Initially, as with its predecessor networks, the system that would evolve into the Internet was primarily for government and government body use.

However, interest in commercial use of the Internet quickly became a commonly debated topic. Although commercial use was forbidden, the exact definition of commercial use was unclear and subjective. UUCPNet and the X.25 IPSS had no such restrictions, which would eventually see the official barring of UUCPNet use of ARPANET and

NSFNET connections. (Some UUCP links still remained connecting to these networks however, as administrators cast a blind eye to their operation.)




## *Number of Internet Hosts Worldwide: 1969–2012*

As a result, during the late 1980s, the first Internet service provider (ISP) companies were formed. Companies like PSINet, UUNET, Netcom, and Portal Software were formed to provide service to the regional research networks and provide alternate network access, UUCP-based email and Usenet News to the public. The first commercial dialup ISP in the United States was The World, which opened in 1989.

In 1992, the U.S. Congress passed the Scientific and Advanced-Technology Act, 42 U.S.C. § 1862(g), which allowed NSF to support access by the research and education communities to computer networks which were not used exclusively for research and education purposes, thus permitting NSFNET to interconnect with commercial networks. This caused controversy within the research and education community, who were concerned commercial use of the network might lead to an Internet that was less responsive to their needs, and within the community of commercial network providers, who felt that government subsidies were giving an unfair advantage to some organizations.

By 1990, ARPANET's goals had been fulfilled and new networking technologies exceeded the original scope and the project came to a close. New network service providers including PSINet, Alternet, CERFNet, ANS CO+RE, and many others were offering network access to commercial customers. NSFNET was no longer the de facto backbone and exchange point of the Internet. The Commercial Internet eXchange (CIX), Metropolitan Area Exchanges (MAEs), and later Network Access Points (NAPs) were becoming the primary interconnections between many networks. The final restrictions on

carrying commercial traffic ended on April 30, 1995 when the National Science Foundation ended its sponsorship of the NSFNET Backbone Service and the service ended. NSF provided initial support for the NAPs and interim support to help the regional research and education networks transition to commercial ISPs. NSF also sponsored the very high speed Backbone Network Service (vBNS) which continued to provide support for the supercomputing centers and research and education in the United States.

## World Wide Web and Introduction of Browsers

The World Wide Web (sometimes abbreviated "www" or "W3") is an information space where documents and other web resources are identified by URIs, interlinked by hypertext links, and can be accessed via the Internet using a web browser and (more recently) web-based applications. It has become known simply as "the Web". As of the 2010s, the World Wide Web is the primary tool billions use to interact on the Internet, and it has changed people's lives immeasurably.

Precursors to the web browser emerged in the form of hyperlinked applications during the mid and late 1980s (the bare concept of hyperlinking had by then existed for some decades). Following these, Tim Berners-Lee is credited with inventing the World Wide Web in 1989 and developing in 1990 both the first web server, and the first web browser, called WorldWideWeb (no spaces) and later renamed Nexus. Many others were soon developed, with Marc Andreessen's 1993 Mosaic (later Netscape), being particularly easy to use and install, and often credited with sparking the internet boom of the 1990s. Today, the major web browsers are Firefox, Internet Explorer, Google Chrome, Opera and Safari.

A boost in web users was triggered in September 1993 by NCSA Mosaic, a graphical browser which eventually ran on several popular office and home computers. This was the first web browser aiming to bring multimedia content to non-technical users, and therefore included images and text on the same page, unlike previous browser designs; its founder, Marc Andreessen, also established the company that in 1994, released Netscape Navigator, which resulted in one of the early browser wars, when it ended up in a competition for dominance (which it lost) with Microsoft Windows' Internet Explorer. Commercial use restrictions were lifted in 1995. The online service America Online (AOL) offered their users a connection to the Internet via their own internal browser.

## Use In Wider Society 1990s to Early 2000s (Web 1.0)

During the first decade or so of the public internet, the immense changes it would eventually enable in the 2000s were still nascent. In terms of providing context for this period, mobile cellular devices ("smartphones" and other cellular devices) which today provide near-universal access, were used for business and not a routine household item owned by parents and children worldwide. Social media in the modern sense had yet to come into existence, laptops were bulky and most households did not have computers. Data rates were slow and most people lacked means to video or digitize video so websites such as YouTube did not yet exist, media storage was transitioning slowly from analog tape to digital optical discs (DVD and to an extent still, floppy disc to CD). Enabling

technologies used from the early 2000s such as PHP, modern Javascript and Java, technologies such as AJAX, HTML 4 (and its emphasis on CSS), and various software frameworks, which enabled and simplified speed of web development, largely awaited invention and their eventual widespread adoption.

The Internet was widely used for mailing lists, emails, e-commerce and early popular online shopping (Amazon and eBay for example), online forums and bulletin boards, and personal websites and blogs, and use was growing rapidly, but by more modern standards the systems used were static and lacked widespread social engagement. It awaited a number of events in the early 2000s to change from a communications technology to gradually develop into a key part of global society's infrastructure.

Typical design elements of these "Web 1.0" era websites included: Static pages instead of dynamic HTML; content served from filesystems instead of relational databases; pages built using Server Side Includes or CGI instead of a web application written in a dynamic programming language; HTML 3.2-era structures such as frames and tables to create page layouts; online guestbooks; overuse of GIF buttons and similar small graphics promoting particular items; and HTML forms sent via email. (Support for server side scripting was rare on shared servers so the usual feedback mechanism was via email, using mailto forms and their email program.

During the period 1997 to 2001, the first speculative investment bubble related to the Internet took place, in which «dot-com" companies (referring to the ".com" top level domain used by businesses) were propelled to exceedingly high valuations as investors rapidly stoked stock values, followed by a market crash; the first dot-com bubble. However this only temporarily slowed enthusiasm and growth, which quickly recovered and continued to grow.

The changes that would propel the Internet into its place as a social system took place during a relatively short period of no more than five years, starting from around 2004. They included:

- The call to "Web 2.0" in 2004 (first suggested in 1999),
- Accelerating adoption and commoditization among households of, and familiarity with, the necessary hardware (such as computers).
- Accelerating storage technology and data access speeds – hard drives emerged, took over from far smaller, slower floppy discs, and grew from megabytes to gigabytes (and by around 2010, terabytes), RAM from hundreds of kilobytes to gigabytes as typical amounts on a system, and Ethernet, the enabling technology for TCP/IP, moved from common speeds of kilobits to tens of megabits per second, to gigabits per second.
- High speed Internet and wider coverage of data connections, at lower prices, allowing larger traffic rates, more reliable simpler traffic, and traffic from more locations,
- The gradually accelerating perception of the ability of computers to create new means and approaches to communication, the emergence of social media and websites such as Twitter and Facebook to their later prominence, and global collaborations such as Wikipedia (which existed before but gained prominence as a result), and shortly after (approximately 2007–2008 onward):

- The mobile revolution, which provided access to the Internet to much of human society of all ages, in their daily lives, and allowed them to share, discuss, and continually update, inquire, and respond.
- Non-volatile RAM rapidly grew in size and reliability, and decreased in price, becoming a commodity capable of enabling high levels of computing activity on these small handheld devices as well as solid-state drives (SSD).
- An emphasis on power efficient processor and device design, rather than purely high processing power; one of the beneficiaries of this was ARM, a British company which had focused since the 1980s on powerful but low cost simple microprocessors. ARM rapidly gained dominance in the market for mobile and embedded devices.

With the call to Web 2.0, the period up to around 2004–2005 was retrospectively named and described by some as Web 1.0.

## *Web 2.0*

The term "Web 2.0" describes websites that emphasize user-generated content (including user-to-user interaction), usability, and interoperability. It first appeared in a January 1999 article called "Fragmented Future" written by Darcy DiNucci, a consultant on electronic information design, where she wrote:

"The Web we know now, which loads into a browser window in essentially static screenfuls, is only an embryo of the Web to come. The first glimmerings of Web 2.0 are beginning to appear, and we are just starting to see how that embryo might develop. The Web will be understood not as screenfuls of text and graphics but as a transport mechanism, the ether through which interactivity happens. It willappear on your computer screen,on your TV setyour car dashboardyour cell phonehand-held game machinesmaybe even your microwave oven."

The term resurfaced during 2002 – 2004, and gained prominence in late 2004 following presentations by Tim O'Reilly and Dale Dougherty at the first Web 2.0 Conference. In their opening remarks, John Battelle and Tim O'Reilly outlined their definition of the "Web as Platform", where software applications are built upon the Web as opposed to upon the desktop. The unique aspect of this migration, they argued, is that "customers are building your business for you". They argued that the activities of users generating content (in the form of ideas, text, videos, or pictures) could be "harnessed" to create value.

Web 2.0 does not refer to an update to any technical specification, but rather to cumulative changes in the way Web pages are made and used. Web 2.0 describes an approach, in which sites focus substantially upon allowing users to interact and collaborate with each other in a social media dialogue as creators of user-generated content in a virtual community, in contrast to Web sites where people are limited to the passive viewing of content. Examples of Web 2.0 include social networking sites, blogs, wikis, folksonomies, video sharing sites, hosted services, Web applications, and mashups. Terry Flew, in his 3rd Edition of *New Media* described what he believed to characterize the differences between Web 1.0 and Web 2.0:

"[The] move from personal websites to blogs and blog site aggregation, from publishing to participation, from web content as the outcome of large up-front investment to an ongoing and interactive process, and from content management systems to links based on tagging (folksonomy)".

This era saw several household names gain prominence through their community-oriented operation – YouTube, Twitter, Facebook, Reddit and Wikipedia being some examples.

## The Mobile Revolution

The process of change generally described as "Web 2.0" was itself greatly accelerated and transformed only a short time later by the increasing growth in mobile devices. This mobile revolution meant that computers in the form of smartphones became something many people used, took with them everywhere, communicated with, used for photographs and videos they instantly shared or to shop or seek information "on the move" – and used socially, as opposed to items on a desk at home or just used for work.

Location-based services, services using location and other sensor information, and crowdsourcing (frequently but not always location based), became common, with posts tagged by location, or websites and services becoming location aware. Mobile-targeted websites (such as "m.website.com") became common, designed especially for the new devices used. Netbooks, ultrabooks, widespread 4G and Wi-Fi, and mobile chips capable or running at nearly the power of desktops from not many years before on far lower power usage, became enablers of this stage of Internet development, and the term "App" emerged (short for "Application program" or "Program") as did the "App store".

## Networking in Outer Space

The first Internet link into low earth orbit was established on January 22, 2010 when astronaut T. J. Creamer posted the first unassisted update to his Twitter account from the International Space Station, marking the extension of the Internet into space. (Astronauts at the ISS had used email and Twitter before, but these messages had been relayed to the ground through a NASA data link before being posted by a human proxy.) This personal Web access, which NASA calls the Crew Support LAN, uses the space station's high-speed Ku band microwave link. To surf the Web, astronauts can use a station laptop computer to control a desktop computer on Earth, and they can talk to their families and friends on Earth using Voice over IP equipment.

Communication with spacecraft beyond earth orbit has traditionally been over point-to-point links through the Deep Space Network. Each such data link must be manually scheduled and configured. In the late 1990s NASA and Google began working on a new network protocol, Delay-tolerant networking (DTN) which automates this process, allows networking of spaceborne transmission nodes, and takes the fact into account that spacecraft can temporarily lose contact because they move behind the Moon or planets, or because space weather disrupts the connection. Under such conditions, DTN retransmits data packages instead of dropping them, as the standard TCP/IP Internet Protocol does.

NASA conducted the first field test of what it calls the "deep space internet" in November 2008. Testing of DTN-based communications between the International Space Station and Earth (now termed Disruption-Tolerant Networking) has been ongoing since March 2009, and is scheduled to continue until March 2014.

This network technology is supposed to ultimately enable missions that involve multiple spacecraft where reliable inter-vessel communication might take precedence over vessel-to-earth downlinks. According to a February 2011 statement by Google's Vint Cerf, the so-called "Bundle protocols" have been uploaded to NASA's EPOXI mission spacecraft (which is in orbit around the Sun) and communication with Earth has been tested at a distance of approximately 80 light seconds.

## Internet Governance

As a globally distributed network of voluntarily interconnected autonomous networks, the Internet operates without a central governing body. It has no centralized governance for either technology or policies, and each constituent network chooses what technologies and protocols it will deploy from the voluntary technical standards that are developed by the Internet Engineering Task Force (IETF). However, throughout its entire history, the Internet system has had an "Internet Assigned Numbers Authority" (IANA) for the allocation and assignment of various technical identifiers needed for the operation of the Internet. The Internet Corporation for Assigned Names and Numbers (ICANN) provides oversight and coordination for two principal name spaces in the Internet, the Internet Protocol address space and the Domain Name System.

### *Nic, Internic, Iana and Icann*

The IANA function was originally performed by USC Information Sciences Institute (ISI), and it delegated portions of this responsibility with respect to numeric network and autonomous system identifiers to the Network Information Center (NIC) at Stanford Research Institute (SRI International) in Menlo Park, California. ISI's Jonathan Postel managed the IANA, served as RFC Editor and performed other key roles until his premature death in 1998.

As the early ARPANET grew, hosts were referred to by names, and a HOSTS. TXT file would be distributed from SRI International to each host on the network. As the network grew, this became cumbersome. A technical solution came in the form of the Domain Name System, created by ISI's Paul Mockapetris in 1983. The Defense Data Network—Network Information Center (DDN-NIC) at SRI handled all registration services, including the top-level domains (TLDs) of .mil, .gov, .edu, .org, .net, .com and .us, root nameserver administration and Internet number assignments under a United States Department of Defense contract. In 1991, the Defense Information Systems Agency (DISA) awarded the administration and maintenance of DDN-NIC (managed by SRI up until this point) to Government Systems, Inc., who subcontracted it to the small private sector Network Solutions, Inc.

The increasing cultural diversity of the Internet also posed administrative challenges for centralized management of the IP addresses. In October 1992, the Internet Engineering

Task Force (IETF) published RFC 1366, which described the "growth of the Internet and its increasing globalization" and set out the basis for an evolution of the IP registry process, based on a regionally distributed registry model. This document stressed the need for a single Internet number registry to exist in each geographical region of the world (which would be of "continental dimensions"). Registries would be "unbiased and widely recognized by network providers and subscribers" within their region. The RIPE Network Coordination Centre (RIPE NCC) was established as the first RIR in May 1992. The second RIR, the Asia Pacific Network Information Centre (APNIC), was established in Tokyo in 1993, as a pilot project of the Asia Pacific Networking Group.

Since at this point in history most of the growth on the Internet was coming from non-military sources, it was decided that the Department of Defense would no longer fund registration services outside of the .mil TLD. In 1993 the U.S. National Science Foundation, after a competitive bidding process in 1992, created the InterNIC to manage the allocations of addresses and management of the address databases, and awarded the contract to three organizations. Registration Services would be provided by Network Solutions; Directory and Database Services would be provided by AT&T; and Information Services would be provided by General Atomics.

Over time, after consultation with the IANA, the IETF, RIPE NCC, APNIC, and the Federal Networking Council (FNC), the decision was made to separate the management of domain names from the management of IP numbers. Following the examples of RIPE NCC and APNIC, it was recommended that management of IP address space then administered by the InterNIC should be under the control of those that use it, specifically the ISPs, end-user organizations, corporate entities, universities, and individuals. As a result, the American Registry for Internet Numbers (ARIN) was established as in December 1997, as an independent, not-for-profit corporation by direction of the National Science Foundation and became the third Regional Internet Registry.

In 1998, both the IANA and remaining DNS-related InterNIC functions were reorganized under the control of ICANN, a California non-profit corporation contracted by the United States Department of Commerce to manage a number of Internet-related tasks. As these tasks involved technical coordination for two principal Internet name spaces (DNS names and IP addresses) created by the IETF, ICANN also signed a memorandum of understanding with the IAB to define the technical work to be carried out by the Internet Assigned Numbers Authority. The management of Internet address space remained with the regional Internet registries, which collectively were defined as a supporting organization within the ICANN structure. ICANN provides central coordination for the DNS system, including policy coordination for the split registry / registrar system, with competition among registry service providers to serve each top-level-domain and multiple competing registrars offering DNS services to end-users.

## *Internet Engineering Task Force*

The Internet Engineering Task Force (IETF) is the largest and most visible of several loosely related ad-hoc groups that provide technical direction for the Internet, including the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG), and the Internet Research Task Force (IRTF).

The IETF is a loosely self-organized group of international volunteers who contribute to the engineering and evolution of Internet technologies. It is the principal body engaged in the development of new Internet standard specifications. Much of the work of the IETF is organized into *Working Groups*. Standardization efforts of the Working Groups are often adopted by the Internet community, but the IETF does not control or patrol the Internet.

The IETF grew out of quarterly meeting of U.S. government-funded researchers, starting in January 1986. Non-government representatives were invited by the fourth IETF meeting in October 1986. The concept of Working Groups was introduced at the fifth meeting in February 1987. The seventh meeting in July 1987 was the first meeting with more than one hundred attendees. In 1992, the Internet Society, a professional membership society, was formed and IETF began to operate under it as an independent international standards body. The first IETF meeting outside of the United States was held in Amsterdam, The Netherlands, in July 1993. Today, the IETF meets three times per year and attendance has been as high as ca. 2,000 participants. Typically one in three IETF meetings are held in Europe or Asia. The number of non-US attendees is typically ca. 50%, even at meetings held in the United States.

The IETF is not a legal entity, has no governing board, no members, and no dues. The closest status resembling membership is being on an IETF or Working Group mailing list. IETF volunteers come from all over the world and from many different parts of the Internet community. The IETF works closely with and under the supervision of the Internet Engineering Steering Group (IESG) and the Internet Architecture Board (IAB).The Internet Research Task Force (IRTF) and the Internet Research Steering Group (IRSG), peer activities to the IETF and IESG under the general supervision of the IAB, focus on longer term research issues.

## Request for Comments

Request for Comments (RFCs) are the main documentation for the work of the IAB, IESG, IETF, and IRTF. RFC 1, “Host Software”, was written by Steve Crocker at UCLA in April 1969, well before the IETF was created. Originally they were technical memos documenting aspects of ARPANET development and were edited by Jon Postel, the first RFC Editor.

RFCs cover a wide range of information from proposed standards, draft standards, full standards, best practices, experimental protocols, history, and other informational topics. RFCs can be written by individuals or informal groups of individuals, but many are the product of a more formal Working Group. Drafts are submitted to the IESG either by individuals or by the Working Group Chair. An RFC Editor, appointed by the IAB, separate from IANA, and working in conjunction with the IESG, receives drafts from the IESG and edits, formats, and publishes them. Once an RFC is published, it is never revised. If the standard it describes changes or its information becomes obsolete, the revised standard or updated information will be re-published as a new RFC that “obsoletes” the original.

### The Internet Society

The Internet Society (ISOC) is an international, non-profit organization founded during 1992 "to assure the open development, evolution and use of the Internet for the benefit of all people throughout the world". With offices near Washington, DC, USA, and in Geneva, Switzerland, ISOC has a membership base comprising more than 80 organizational and more than 50,000 individual members. Members also form "chapters" based on either common geographical location or special interests. There are currently more than 90 chapters around the world. ISOC provides financial and organizational support to and promotes the work of the standards settings bodies for which it is the organizational home: the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), the Internet Engineering Steering Group (IESG), and the Internet Research Task Force (IRTF). ISOC also promotes understanding and appreciation of the Internet model of open, transparent processes and consensus-based decision-making.

### Globalization and Internet Governance in the 21st Century

Since the 1990s, the Internet's governance and organization has been of global importance to governments, commerce, civil society, and individuals. The organizations which held control of certain technical aspects of the Internet were the successors of the old ARPANET oversight and the current decision-makers in the day-to-day technical aspects of the network. While recognized as the administrators of certain aspects of the Internet, their roles and their decision-making authority are limited and subject to increasing international scrutiny and increasing objections. These objections have led to the ICANN removing themselves from relationships with first the University of Southern California in 2000, and finally in September 2009, gaining autonomy from the US government by the ending of its longstanding agreements, although some contractual obligations with the U.S. Department of Commerce continued.

The IETF, with financial and organizational support from the Internet Society, continues to serve as the Internet's ad-hoc standards body and issues Request for Comments.

In November 2005, the World Summit on the Information Society, held in Tunis, called for an Internet Governance Forum (IGF) to be convened by United Nations Secretary General. The IGF opened an ongoing, non-binding conversation among stakeholders representing governments, the private sector, civil society, and the technical and academic communities about the future of Internet governance. The first IGF meeting was held in October/November 2006 with follow up meetings annually thereafter. Since WSIS, the term "Internet governance" has been broadened beyond narrow technical concerns to include a wider range of Internet-related policy issues.

## Politicization of the Internet

Due to its prominence and immediacy as an effective means of mass communication, the Internet has also become more politicized as it has grown. This has led in turn, to discourses and activities that would once have taken place in other ways, migrating to being mediated by internet.

Examples include political activities such as public protest and canvassing of support and votes, but also –

- The spreading of ideas and opinions;
- Recruitment of followers, and "coming together" of members of the public, for ideas, products, and causes;
- Providing and widely distributing and sharing information that might be deemed sensitive or relates to whistleblowing (and efforts by specific countries to prevent this by censorship);
- Criminal activity and terrorism (and resulting law enforcement use, together with its facilitation by mass surveillance).

## *Net Neutrality*

On April 23, 2014, the Federal Communications Commission (FCC) was reported to be considering a new rule that would permit Internet service providers to offer content providers a faster track to send content, thus reversing their earlier net neutrality position. A possible solution to net neutrality concerns may be municipal broadband, according to Professor Susan Crawford, a legal and technology expert at Harvard Law School. On May 15, 2014, the FCC decided to consider two options regarding Internet services: first, permit fast and slow broadband lanes, thereby compromising net neutrality; and second, reclassify broadband as a telecommunication service, thereby preserving net neutrality. On November 10, 2014, President Obama recommended the FCC reclassify broadband Internet service as a telecommunications service in order to preserve net neutrality. On January 16, 2015, Republicans presented legislation, in the form of a U.S. Congress H. R. discussion draft bill, that makes concessions to net neutrality but prohibits the FCC from accomplishing the goal or enacting any further regulation affecting Internet service providers (ISPs). On January 31, 2015, AP News reported that the FCC will present the notion of applying ("with some caveats") Title II (common carrier) of the Communications Act of 1934 to the internet in a vote expected on February 26, 2015.Adoption of this notion would reclassify internet service from one of information to one of telecommunications and, according to Tom Wheeler, chairman of the FCC, ensure net neutrality. The FCC is expected to enforce net neutrality in its vote, according to the New York Times.

On February 26, 2015, the FCC ruled in favor of net neutrality by applying Title II (common carrier) of the Communications Act of 1934 and Section 706 of the Telecommunications act of 1996 to the Internet. The FCC Chairman, Tom Wheeler, commented, "This is no more a plan to regulate the Internet than the First Amendment is a plan to regulate free speech. They both stand for the same concept."

On March 12, 2015, the FCC released the specific details of the net neutrality rules. On April 13, 2015, the FCC published the final rule on its new "Net Neutrality" regulations.

# Use and Culture

## Email and Usenet

E-mail has often been called the killer application of the Internet. It predates the Internet, and was a crucial tool in creating it. Email started in 1965 as a way for multiple users of a time-sharing mainframe computer to communicate. Although the history is undocumented, among the first systems to have such a facility were the System Development Corporation (SDC) Q32 and the Compatible Time-Sharing System (CTSS) at MIT.

The ARPANET computer network made a large contribution to the evolution of electronic mail. An experimental inter-system transferred mail on the ARPANET shortly after its creation. In 1971 Ray Tomlinson created what was to become the standard Internet electronic mail addressing format, using the @ sign to separate mailbox names from host names.

A number of protocols were developed to deliver messages among groups of time-sharing computers over alternative transmission systems, such as UUCP and IBM's VNET email system. Email could be passed this way between a number of networks, including ARPANET, BITNET and NSFNET, as well as to hosts connected directly to other sites via UUCP. See the history of SMTP protocol.

In addition, UUCP allowed the publication of text files that could be read by many others. The News software developed by Steve Daniel and Tom Truscott in 1979 was used to distribute news and bulletin board-like messages. This quickly grew into discussion groups, known as newsgroups, on a wide range of topics. On ARPANET and NSFNET similar discussion groups would form via mailing lists, discussing both technical issues and more culturally focused topics (such as science fiction, discussed on the sflovers mailing list).

During the early years of the Internet, email and similar mechanisms were also fundamental to allow people to access resources that were not available due to the absence of online connectivity. UUCP was often used to distribute files using the ‹alt. binary' groups. Also, FTP e-mail gateways allowed people that lived outside the US and Europe to download files using ftp commands written inside email messages. The file was encoded, broken in pieces and sent by email; the receiver had to reassemble and decode it later, and it was the only way for people living overseas to download items such as the earlier Linux versions using the slow dial-up connections available at the time. After the popularization of the Web and the HTTP protocol such tools were slowly abandoned.

## From Gopher to the WWW

As the Internet grew through the 1980s and early 1990s, many people realized the increasing need to be able to find and organize files and information. Projects such as Archie, Gopher, WAIS, and the FTP Archive list attempted to create ways to organize distributed data. In the early 1990s, Gopher, invented by Mark P. McCahill offered a viable alternative to the World Wide Web. However, in 1993 the World Wide Web saw many advances to indexing and ease of access through search engines, which often neglected Gopher and

Gopherspace. As popularity increased through ease of use, investment incentives also grew until in the middle of 1994 the WWW's popularity gained the upper hand. Then it became clear that Gopher and the other projects were doomed fall short.

One of the most promising user interface paradigms during this period was hypertext. The technology had been inspired by Vannevar Bush's "Memex" and developed through Ted Nelson's research on Project Xanadu and Douglas Engelbart's research on NLS. Many small self-contained hypertext systems had been created before, such as Apple Computer's HyperCard (1987). Gopher became the first commonly used hypertext interface to the Internet. While Gopher menu items were examples of hypertext, they were not commonly perceived in that way.




This NeXT Computer was used by Sir Tim Berners-Lee at CERN and became the world's first Web server.

In 1989, while working at CERN, Tim Berners-Lee invented a network-based implementation of the hypertext concept. By releasing his invention to public use, he ensured the technology would become widespread. For his work in developing the World Wide Web, Berners-Lee received the Millennium technology prize in 2004. One early popular web browser, modeled after HyperCard, was ViolaWWW.

A turning point for the World Wide Web began with the introduction of the Mosaic web browser in 1993, a graphical browser developed by a team at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign (NCSA-UIUC), led by Marc Andreessen. Funding for Mosaic came from the *High-Performance Computing and Communications Initiative*, a funding program initiated by the *High Performance Computing and Communication Act of 1991* also known as the *Gore Bill*.Mosaic's graphical interface soon became more popular than Gopher, which at the time was primarily text-based, and the WWW became the preferred interface for accessing the Internet. (Gore's reference to his role in "creating the Internet", however, was ridiculed in his presidential election campaign. See the full article Al Gore and information technology).

Mosaic was superseded in 1994 by Andreessen's Netscape Navigator, which replaced Mosaic as the world's most popular browser. While it held this title for some time, eventually competition from Internet Explorer and a variety of other browsers almost completely displaced it. Another important event held on January 11, 1994, was *The Superhighway Summit* at UCLA's Royce Hall. This was the "first public conference bringing together all of the major industry, government and academic leaders in the field [and] also began the national dialogue about the *Information Superhighway* and its implications."

*24 Hours in Cyberspace*, "the largest one-day online event" (February 8, 1996) up to that date, took place on the then-active website, *cyber24.com.* It was headed by photographer Rick Smolan. A photographic exhibition was unveiled at the Smithsonian Institution's National Museum of American History on January 23, 1997, featuring 70 photos from the project.

## Search Engines

Even before the World Wide Web, there were search engines that attempted to organize the Internet. The first of these was the Archie search engine from McGill University in 1990, followed in 1991 by WAIS and Gopher. All three of those systems predated the invention of the World Wide Web but all continued to index the Web and the rest of the Internet for several years after the Web appeared. There are still Gopher servers as of 2006, although there are a great many more web servers.

As the Web grew, search engines and Web directories were created to track pages on the Web and allow people to find things. The first full-text Web search engine was WebCrawler in 1994. Before WebCrawler, only Web page titles were searched. Another early search engine, Lycos, was created in 1993 as a university project, and was the first to achieve commercial success. During the late 1990s, both Web directories and Web search engines were popular—Yahoo! (founded 1994) and Altavista (founded 1995) were the respective industry leaders. By August 2001, the directory model had begun to give way to search engines, tracking the rise of Google (founded 1998), which had developed new approaches to relevancy ranking. Directory features, while still commonly available, became after-thoughts to search engines.

Database size, which had been a significant marketing feature through the early 2000s, was similarly displaced by emphasis on relevancy ranking, the methods by which search engines attempt to sort the best results first. Relevancy ranking first became a major issue circa 1996, when it became apparent that it was impractical to review full lists of results. Consequently, algorithms for relevancy ranking have continuously improved. Google's PageRank method for ordering the results has received the most press, but all major search engines continually refine their ranking methodologies with a view toward improving the ordering of results. As of 2006, search engine rankings are more important than ever, so much so that an industry has developed ("search engine optimizers", or "SEO") to help web-developers improve their search ranking, and an entire body of case law has developed around matters that affect search engine rankings, such as use of trademarks in metatags. The sale of search rankings by some search engines has also created controversy among librarians and consumer advocates.

On June 3, 2009, Microsoft launched its new search engine, Bing. The following month Microsoft and Yahoo! announced a deal in which Bing would power Yahoo! Search.

## File Sharing

Resource or file sharing has been an important activity on computer networks from well before the Internet was established and was supported in a variety of ways including bulletin board systems (1978), Usenet (1980), Kermit (1981), and many others. The File Transfer Protocol (FTP) for use on the Internet was standardized in 1985 and is still in use today. A variety of tools were developed to aid the use of FTP by helping users discover files they might want to transfer, including the Wide Area Information Server (WAIS) in 1991, Gopher in 1991, Archie in 1991, Veronica in 1992, Jughead in 1993, Internet Relay Chat (IRC) in 1988, and eventually the World Wide Web (WWW) in 1991 with Web directories and Web search engines.

In 1999, Napster became the first peer-to-peer file sharing system. Napster used a central server for indexing and peer discovery, but the storage and transfer of files was decentralized. A variety of peer-to-peer file sharing programs and services with different levels of decentralization and anonymity followed, including: Gnutella, eDonkey2000, and Freenet in 2000, FastTrack, Kazaa, Limewire, and BitTorrent in 2001, and Poisoned in 2003.

All of these tools are general purpose and can be used to share a wide variety of content, but sharing of music files, software, and later movies and videos are major uses. And while some of this sharing is legal, large portions are not. Lawsuits and other legal actions caused Napster in 2001, eDonkey2000 in 2005, Kazaa in 2006, and Limewire in 2010 to shut down or refocus their efforts. The Pirate Bay, founded in Sweden in 2003, continues despite a trial and appeal in 2009 and 2010 that resulted in jail terms and large fines for several of its founders. File sharing remains contentious and controversial with charges of theft of intellectual property on the one hand and charges of censorship on the other.

## Dot-Com Bubble

Suddenly the low price of reaching millions worldwide, and the possibility of selling to or hearing from those people at the same moment when they were reached, promised to overturn established business dogma in advertising, mail-order sales, customer relationship management, and many more areas. The web was a new killer app—it could bring together unrelated buyers and sellers in seamless and low-cost ways. Entrepreneurs around the world developed new business models, and ran to their nearest venture capitalist. While some of the new entrepreneurs had experience in business and economics, the majority were simply people with ideas, and did not manage the capital influx prudently. Additionally, many dot-com business plans were predicated on the assumption that by using the Internet, they would bypass the distribution channels of existing businesses and therefore not have to compete with them; when the established businesses with strong existing brands developed their own Internet presence, these hopes were shattered, and

the newcomers were left attempting to break into markets dominated by larger, more established businesses. Many did not have the ability to do so.

The dot-com bubble burst in March 2000, with the technology heavy NASDAQ Composite index peaking at 5,048.62 on March 10 (5,132.52 intraday), more than double its value just a year before. By 2001, the bubble's deflation was running full speed. A majority of the dot-coms had ceased trading, after having burnt through their venture capital and IPO capital, often without ever making a profit. But despite this, the Internet continues to grow, driven by commerce, ever greater amounts of online information and knowledge and social networking.

### *Mobile Phones and the Internet*

The first mobile phone with Internet connectivity was the Nokia 9000 Communicator, launched in Finland in 1996. The viability of Internet services access on mobile phones was limited until prices came down from that model, and network providers started to develop systems and services conveniently accessible on phones. NTT DoCoMo in Japan launched the first mobile Internet service, i-mode, in 1999 and this is considered the birth of the mobile phone Internet services. In 2001, the mobile phone email system by Research in Motion for their BlackBerry product was launched in America. To make efficient use of the small screen and tiny keypad and one-handed operation typical of mobile phones, a specific document and networking model was created for mobile devices, the Wireless Application Protocol (WAP). Most mobile device Internet services operate using WAP. The growth of mobile phone services was initially a primarily Asian phenomenon with Japan, South Korea and Taiwan all soon finding the majority of their Internet users accessing resources by phone rather than by PC. Developing countries followed, with India, South Africa, Kenya, Philippines, and Pakistan all reporting that the majority of their domestic users accessed the Internet from a mobile phone rather than a PC. The European and North American use of the Internet was influenced by a large installed base of personal computers, and the growth of mobile phone Internet access was more gradual, but had reached national penetration levels of 20–30% in most Western countries.The cross-over occurred in 2008, when more Internet access devices were mobile phones than personal computers. In many parts of the developing world, the ratio is as much as 10 mobile phone users to one PC user.

## Web Technologies

Web pages were initially conceived as structured documents based upon Hypertext Markup Language (HTML) which can allow access to images, video, and other content. Hyperlinks in the page permit users to navigate to other pages. In the earliest browsers, images opened in a separate "helper" application. Marc Andreessen's 1993 Mosaic and 1994 Netscape introduced mixed text and images for non-technical users. HTML evolved during the 1990s, leading to HTML 4 which introduced large elements of CSS styling and, later, extensions to allow browser code to make calls and ask for content from servers in a structured way (AJAX).

## Historiography

There are nearly insurmountable problems in supplying a historiography of the Internet's development. The process of digitization represents a twofold challenge both for historiography in general and, in particular, for historical communication research. A sense of the difficulty in documenting early developments that led to the internet can be gathered from the quote:

"The Arpanet period is somewhat well documented because the corporation in charge – BBN – left a physical record. Moving into the NSFNET era, it became an extraordinarily decentralized process. The record exists in people's basements, in closets. ... So much of what happened was done verbally and on the basis of individual trust."

—Doug Gale (2007)

## REFERENCES


1. Kim, Byung-Keun (2005). Internationalising the Internet the Co-evolution of Influence and Technology. Edward Elgar. pp. 51–55. ISBN 1845426754.
2. "Brief History of the Internet". Internet Society. Retrieved 9 April 2016. It happened that the work at MIT (1961-1967), at RAND (1962-1965), and at NPL (1964-1967) had all proceeded in parallel without any of the researchers knowing about the other work. The word "packet" was adopted from the work at NPL
3. "Turing's Legacy: A History of Computing at the National Physical Laboratory 1945–1995", David M. Yates, National Museum of Science and Industry, 1997, pages 126–146, ISBN 0901805947. Retrieved 19 May 2015.
4. "Data Communications at the National Physical Laboratory (1965–1975)", Martin Campbell-Kelly, IEEE Annals of the History of Computing, Volume 9 Issue 3–4 (July–Sept 1987), pages 221–247. Retrieved 18 May 2015.
5. "The First ISP". Indra.com. August 13, 1992. Archived from the original on March 5, 2016. Retrieved 2015-10-17.
6. Couldry, Nick (2012). Media, Society, World: Social Theory and Digital Media Practice. London: Polity Press. p. 2.
7. "The World's Technological Capacity to Store, Communicate, and Compute Information", Martin Hilbert and Priscila López (2011), Science (journal), 332(6025), 60–65; free access to the article through here: martinhilbert.net/WorldInfoCapacity.html
8. J. C. R. Licklider (March 1960). "Man-Computer Symbiosis". IRE Transactions on Human Factors in Electronics. HFE-1: 4–11.
9. J. C. R. Licklider and Welden Clark (August 1962). "On-Line Man-Computer Communication" (PDF). AIEE-IRE '62 (Spring): 113–128.
10. Licklider, J. C. R. (23 April 1963). "Topics for Discussion at the Forthcoming Meeting, Memorandum For: Members and Affiliates of the Intergalactic Computer Network". Washington, D.C.: Advanced Research Projects Agency. Retrieved 2013-01-26.

11. Robert Taylor in an interview with John Markoff (December 20, 1999). "An Internet Pioneer Ponders the Next Revolution". The New York Times. Retrieved November 25, 2005.
12. "J.C.R. Licklider and the Universal Network". The Internet. 2000.
13. Baran, Paul (May 27, 1960). "Reliable Digital Communications Using Unreliable Network Repeater Nodes" (PDF). The RAND Corporation: 1. Retrieved July 25, 2012.
14. Ruthfield, Scott (September 1995). "The Internet's History and Development From Wartime Tool to the Fish-Cam". Crossroads. 2 (1). pp. 2–4. doi:10.1145/332198.332202. Archived from the original on October 18, 2007. Retrieved April 1, 2016.
15. "About Rand". Paul Baran and the Origins of the Internet. Retrieved July 25, 2012.
16. Strickland, Jonathan. "How ARPANET Works".
17. Gromov, Gregory (1995). "Roads and Crossroads of Internet History".
18. Hafner, Katie (1998). Where Wizards Stay Up Late: The Origins Of The Internet. Simon & Schuster. ISBN 0-684-83267-4.
19. Ronda Hauben (2001). "From the ARPANET to the Internet". Retrieved May 28, 2009.
20. Postel, J. (November 1981). "The General Plan". NCP/TCP transition plan. IETF. p. 2. RFC 801. Retrieved February 1, 2011.
21. "NORSAR and the Internet". NORSAR. Retrieved June 5, 2009.
22. Ward, Mark (October 29, 2009). "Celebrating 40 years of the net". BBC News.
23. "Donald Davies". thocp.net.
24. "Donald Davies". internethalloffame.org.
25. The Merit Network, Inc. is an independent non-profit 501(c)(3) corporation governed by Michigan's public universities. Merit receives administrative services under an agreement with the University of Michigan.
26. A Chronicle of Merit's Early History, John Mulcahy, 1989, Merit Network, Ann Arbor, Michigan
27. Merit Network Timeline: 1970–1979, Merit Network, Ann Arbor, Michigan
28. Merit Network Timeline: 1980–1989, Merit Network, Ann Arbor, Michigan
29. "A Technical History of CYCLADES". Technical Histories of the Internet & other Network Protocols. Computer Science Department, University of Texas Austin.
30. "The Cyclades Experience: Results and Impacts", Zimmermann, H., Proc. IFIP'77 Congress, Toronto, August 1977, pp. 465–469
31. tsbedh. "History of X.25, CCITT Plenary Assemblies and Book Colors". Itu. int. Retrieved June 5, 2009.
32. "Events in British Telecomms History". Events in British TelecommsHistory. Archived from the original on April 5, 2003. Retrieved November 25, 2005.

33. UUCP Internals Frequently Asked Questions
34. Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff (2003). "A Brief History of Internet". Retrieved May 28, 2009.
35. "Computer History Museum and Web History Center Celebrate 30th Anniversary of Internet Milestone". Retrieved November 22, 2007.
36. Ogg, Erica (2007-11-08). "'Internet van' helped drive evolution of the Web". CNET. Retrieved 2011-11-12.
37. Jon Postel, NCP/TCP Transition Plan, RFC 801
38. David Roessner; Barry Bozeman; Irwin Feller; Christopher Hill; Nils Newman (1997). "The Role of NSF's Support of Engineering in Enabling Technological Innovation". Retrieved May 28, 2009.
39. "RFC 675 – Specification of internet transmission control program". Tools.ietf.org. Retrieved May 28, 2009.
40. Tanenbaum, Andrew S. (1996). Computer Networks. Prentice Hall. ISBN 0-13-394248-1.
41. Hauben, Ronda (2004). "The Internet: On its International Origins and Collaborative Vision". Amateur Computerist. 12 (2). Retrieved May 29, 2009.
42. "Internet Access Provider Lists". Retrieved May 10, 2012.
43. "RFC 1871 – CIDR and Classful Routing". Tools.ietf.org. Retrieved May 28, 2009.
44. Ben Segal (1995). "A Short History of Internet Protocols at CERN".
45. "A Brief History of the Internet in Korea (2005) - 한국 인터넷 역사 프로젝트". sites.google.com. Retrieved 2016-05-30.
46. "Three decades since the introduction of the internet in Korea". world.kbs.co.kr. Retrieved 2016-05-30.
47. "Internet History in Asia". 16th APAN Meetings/Advanced Network Conference in Busan. Retrieved December 25, 2005.
48. "Percentage of Individuals using the Internet 2000–2012", International Telecommunications Union (Geneva), June 2013, retrieved 22 June 2013
49. "Fixed (wired)-broadband subscriptions per 100 inhabitants 2012", Dynamic Report, ITU ITC EYE, International Telecommunication Union. Retrieved on 29 June 2013.
50. "Active mobile-broadband subscriptions per 100 inhabitants 2012", Dynamic Report, ITU ITC EYE, International Telecommunication Union. Retrieved on 29 June 2013.
51. "ICONS webpage". Icons.afrinic.net. Retrieved May 28, 2009.
52. Nepad, Eassy partnership ends in divorce,(South African) Financial Times FMTech, 2007
53. "APRICOT webpage". Apricot.net. May 4, 2009. Retrieved May 28, 2009.

54. "A brief history of the Internet in China". China celebrates 10 years of being connected to the Internet. Retrieved December 25, 2005.
55. "Internet host count history". Internet Systems Consortium. Retrieved May 16, 2012.
56. "The World internet provider". Retrieved May 28, 2009.
57. OGC-00-33R Department of Commerce: Relationship with the Internet Corporation for Assigned Names and Numbers (PDF). Government Accountability Office. July 7, 2000. p. 6.
58. Even after the appropriations act was amended in 1992 to give NSF more flexibility with regard to commercial traffic, NSF never felt that it could entirely do away with its Acceptable Use Policy and its restrictions on commercial traffic, see the response to Recommendation 5 in NSF's response to the Inspector General's review (a April 19, 1993 memo from Frederick Bernthal, Acting Director, to Linda Sundro, Inspector General, that is included at the end of Review of NSFNET, Office of the Inspector General, National Science Foundation, March 23, 1993)
59. Management of NSFNET, a transcript of the March 12, 1992 hearing before the Subcommittee on Science of the Committee on Science, Space, and Technology, U.S. House of Representatives, One Hundred Second Congress, Second Session, Hon. Rick Boucher, subcommittee chairman, presiding
60. "Retiring the NSFNET Backbone Service: Chronicling the End of an Era", Susan R. Harris, Ph.D., and Elise Gerich, ConneXions, Vol. 10, No. 4, April 1996
61. "A Brief History of the Internet".
62. NSF Solicitation 93-52 – Network Access Point Manager, Routing Arbiter, Regional Network Providers, and Very High Speed Backbone Network Services Provider for NSFNET and the NREN(SM) Program, May 6, 1993
63. "What is the difference between the Web and the Internet?". W3C Help and FAQ. W3C. 2009. Retrieved 16 July 2015.
64. "World Wide Web Timeline". Pews Research Center. 11 March 2014. Retrieved 1 August 2015.
65. Dewey, Caitlin (12 March 2014). "36 Ways The Web Has Changed Us". The Washington Post. Retrieved 1 August 2015.
66. "Website Analytics Tool". Retrieved 1 August 2015.
67. "Tim Berners-Lee: WorldWideWeb, the first Web client". W3.org.
68. "Frequently asked questions by the Press – Tim BL". W3.org.
69. "Bloomberg Game Changers: Marc Andreessen". Bloomberg.com. 17 March 2011.
70. "Browser". Mashable. Retrieved 2 September 2011.
71. Vetter, Ronald J. (October 1994). "Mosaic and the World-Wide Web" (PDF). North Dakota State University. Retrieved 20 November 2010.
72. Berners-Lee, Tim. "What were the first WWW browsers?". World Wide Web Consortium. Retrieved 2010-06-15.

73. Viswanathan, Ganesh; Dutt Mathur, Punit; Yammiyavar, Pradeep (March 2010). "From Web 1.0 to Web 2.0 and beyond: Reviewing usability heuristic criteria taking music sites as case studies". IndiaHCI Conference. Mumbai. Retrieved 20 February 2015.
74. Web 1.0 defined – How stuff works
75. "Web 1.0 Revisited – Too many stupid buttons". Complexify.com. Archived February 16, 2006, at the Wayback Machine.
76. "The Right Size of Software".
77. Graham, Paul (November 2005). "Web 2.0". Retrieved 2006-08-02. I first heard the phrase 'Web 2.0' in the name of the Web 2.0 conference in 2004.
78. O'Reilly, Tim (2005-09-30). "What Is Web 2.0". O'Reilly Network. Retrieved 2006-08-06.
79. Strickland, Jonathan (2007-12-28). "How Web 2.0 Works". computer. howstuffworks.com. Retrieved 2015-02-28.
80. DiNucci, Darcy (1999). "Fragmented Future" (PDF). Print. 53 (4): 32.
81. Idehen, Kingsley. 2003. RSS: INJAN (It's not just about news). Blog. Blog Data Space. August 21 OpenLinkSW.com
82. Idehen, Kingsley. 2003. Jeff Bezos Comments about Web Services. Blog. Blog Data Space. September 25. OpenLinkSW.com
83. Knorr, Eric. 2003. The year of Web services. CIO, December 15.
84. "John Robb's Weblog". Jrobb.mindplex.org. Archived from the original on May 16, 2008. Retrieved 2011-02-06.
85. O'Reilly, Tim, and John Battelle. 2004. Opening Welcome: State of the Internet Industry. In San Francisco, California, October 5.
86. 031072208 (2005-10-01). "Web 2.0: Compact Definition". Scholar. googleusercontent.com. Retrieved 2013-06-15.[dead link]
87. Flew, Terry (2008). New Media: An Introduction (3rd ed.). Melbourne: Oxford University Press. p. 19.
88. "Twitter post". January 22, 2010. Archived from the original on March 10, 2013. Retrieved 2013-03-10.
89. NASA Extends the World Wide Web Out Into Space. NASA media advisory M10-012, January 22, 2010. Archived
90. NASA Successfully Tests First Deep Space Internet. NASA media release 08-298, November 18, 2008 Archived
91. Disruption Tolerant Networking for Space Operations (DTN). July 31, 2012
92. "Cerf: 2011 will be proving point for 'InterPlanetary Internet'". Network World interview with Vint Cerf. February 18, 2011. Archivedfrom the original on December 9, 2012.
93. "Internet Architecture". IAB Architectural Principles of the Internet. Retrieved April 10, 2012.

94. "DDN NIC". IAB Recommended Policy on Distributing Internet Identifier Assignment. Retrieved December 26, 2005.
95. Internet Hall of Fame
96. Elizabeth Feinler, IEEE Annals [3B2-9] man2011030074.3d 29/7/011 11:54 Page 74
97. "GSI-Network Solutions". TRANSITION OF NIC SERVICES. Retrieved December 26, 2005.
98. "Thomas v. NSI, Civ. No. 97-2412 (TFH), Sec. I.A. (DCDC April 6, 1998)". Lw.bna.com. Retrieved May 28, 2009.
99. "RFC 1366". Guidelines for Management of IP Address Space. Retrieved April 10, 2012.
100. "Development of the Regional Internet Registry System". Cisco. Retrieved April 10, 2012.
101. "NIS Manager Award Announced". NSF Network information services awards. Retrieved December 25, 2005.
102. "Internet Moves Toward Privatization". www.nsf.gov. 24 June 1997.
103. "RFC 2860". Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority. Retrieved December 26, 2005.
104. "ICANN Bylaws". Retrieved April 10, 2012.
105. "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force", FYI 17 and RFC 4677, P. Hoffman and S. Harris, Internet Society, September 2006
106. "A Mission Statement for the IETF", H. Alvestrand, Internet Society, BCP 95 and RFC 3935, October 2004
107. "An IESG charter", H. Alvestrand, RFC 3710, Internet Society, February 2004
108. "Charter of the Internet Architecture Board (IAB)", B. Carpenter, BCP 39 and RFC 2850, Internet Society, May 2000
109. "IAB Thoughts on the Role of the Internet Research Task Force (IRTF)", S. Floyd, V. Paxson, A. Falk (eds), RFC 4440, Internet Society, March 2006
110. The RFC Series and RFC Editor", L. Daigle, RFC 4844, Internet Society, July 2007
111. "Not All RFCs are Standards", C. Huitema, J. Postel, S. Crocker, RFC 1796, Internet Society, April 1995
112. Internet Society (ISOC) – Introduction to ISOC
113. Internet Society (ISOC) – ISOC's Standards Activities
114. USC/ICANN Transition Agreement
115. ICANN cuts cord to US government, gets broader oversight: ICANN, which oversees the Internet's domain name system, is a private nonprofit that reports to the US Department of Commerce. Under a new agreement, that relationship will change, and ICANN's accountability goes global Nate Anderson, September

30, 2009

116. Rhoads, Christopher (October 2, 2009). "U.S. Eases Grip Over Web Body: Move Addresses Criticisms as Internet Usage Becomes More Global". The Wall Street Journal.
117. Rabkin, Jeremy; Eisenach, Jeffrey (October 2, 2009). "The U.S. Abandons the Internet: Multilateral governance of the domain name system risks censorship and repression". The Wall Street Journal.
118. Mueller, Milton L. (2010). Networks and States: The Global Politics of Internet Governance. MIT Press. p. 67. ISBN 978-0-262-01459-5.
119. Mueller, Milton L. (2010). Networks and States: The Global Politics of Internet Governance. MIT Press. pp. 79–80. ISBN 978-0-262-01459-5.
120. DeNardis, Laura, The Emerging Field of Internet Governance(September 17, 2010). Yale Information Society Project Working Paper Series.
121. Wyatt, Edward (April 23, 2014). "F.C.C., in 'Net Neutrality' Turnaround, Plans to Allow Fast Lane". New York Times. Retrieved 2014-04-23.
122. Staff (April 24, 2014). "Creating a Two-Speed Internet". New York Times. Retrieved 2014-04-25.
123. Carr, David (May 11, 2014). "Warnings Along F.C.C.'s Fast Lane". New York Times. Retrieved 2014-05-11.
124. Crawford, Susan (April 28, 2014). "The Wire Next Time". New York Times. Retrieved 2014-04-28.
125. Staff (May 15, 2014). "Searching for Fairness on the Internet". New York Times. Retrieved 2014-05-15.
126. Wyatt, Edward (May 15, 2014). "F.C.C. Backs Opening Net Rules for Debate". New York Times. Retrieved 2014-05-15.
127. Wyatt, Edward (November 10, 2014). "Obama Asks F.C.C. to Adopt Tough Net Neutrality Rules". New York Times. Retrieved November 15, 2014.
128. NYT Editorial Board (November 14, 2014). "Why the F.C.C. Should Heed President Obama on Internet Regulation". New York Times. Retrieved November 15, 2014.
129. Sepulveda, Ambassador Daniel A. (January 21, 2015). "The World Is Watching Our Net Neutrality Debate, So Let's Get It Right". Wired (website). Retrieved January 20, 2015.
130. Weisman, Jonathan (January 19, 2015). "Shifting Politics of Net Neutrality Debate Ahead of F.C.C. Vote". New York Times. Retrieved January 20, 2015.
131. Staff (January 16, 2015). "H. R. _ 114th Congress, 1st Session [Discussion Draft] – To amend the Communications Act of 1934 to ensure Internet openness..." (PDF). U. S. Congress. Retrieved January 20, 2015.
132. Lohr, Steve (February 2, 2015). "In Net Neutrality Push, F.C.C. Is Expected to Propose Regulating Internet Service as a Utility". New York Times. Retrieved February 2, 2015.

133. Lohr, Steve (February 2, 2015). "F.C.C. Chief Wants to Override State Laws Curbing Community Net Services". New York Times. Retrieved February 2, 2015.
134. Flaherty, Anne (January 31, 2015). "Just whose Internet is it? New federal rules may answer that". Associated Press. Retrieved January 31, 2015.
135. Fung, Brian (January 2, 2015). "Get ready: The FCC says it will vote on net neutrality in February". Washington Post. Retrieved January 2, 2015.
136. Staff (January 2, 2015). "FCC to vote next month on net neutrality rules". Associated Press. Retrieved January 2, 2015.
137. Lohr, Steve (February 4, 2015). "F.C.C. Plans Strong Hand to Regulate the Internet". New York Times. Retrieved February 5, 2015.
138. Wheeler, Tom (February 4, 2015). "FCC Chairman Tom Wheeler: This Is How We Will Ensure Net Neutrality". Wired (magazine). Retrieved February 5, 2015.
139. The Editorial Board (February 6, 2015). "Courage and Good Sense at the F.C.C. – Net Neutrality's Wise New Rules". New York Times. Retrieved February 6, 2015.
140. Weisman, Jonathan (February 24, 2015). "As Republicans Concede, F.C.C. Is Expected to Enforce Net Neutrality". New York Times. Retrieved February 24, 2015.
141. Lohr, Steve (February 25, 2015). "The Push for Net Neutrality Arose From Lack of Choice". New York Times. Retrieved February 25, 2015.
142. Staff (February 26, 2015). "FCC Adopts Strong, Sustainable Rules To Protect The Open Internet" (PDF). Federal Communications Commission. Retrieved February 26, 2015.
143. Ruiz, Rebecca R.; Lohr, Steve (February 26, 2015). "In Net Neutrality Victory, F.C.C. Classifies Broadband Internet Service as a Public Utility". New York Times. Retrieved February 26, 2015.
144. Flaherty, Anne (February 25, 2015). "FACT CHECK: Talking heads skew 'net neutrality' debate". Associated Press. Retrieved February 26, 2015.
145. Liebelson, Dana (February 26, 2015). "Net Neutrality Prevails In Historic FCC Vote". The Huffington Post. Retrieved February 27, 2015.
146. Ruiz, Rebecca R. (March 12, 2015). "F.C.C. Sets Net Neutrality Rules". New York Times. Retrieved March 13, 2015.
147. Sommer, Jeff (March 12, 2015). "What the Net Neutrality Rules Say". New York Times. Retrieved March 13, 2015.
148. FCC Staff (March 12, 2015). "Federal Communications Commission – FCC 15–24 – In the Matter of Protecting and Promoting the Open Internet – GN Docket No. 14-28 – Report and Order on Remand, Declaratory Ruling, and Order" (PDF). Federal Communications Commission. Retrieved March 13, 2015.
149. Reisinger, Don (April 13, 2015). "Net neutrality rules get published – let the lawsuits begin". CNET. Retrieved April 13, 2015.
150. Federal Communications Commission (April 13, 2015). "Protecting and Promoting

the Open Internet – A Rule by the Federal Communications Commission on 04/13/2015". Federal Register. Retrieved April 13, 2015.

151. "The Risks Digest". Great moments in e-mail history. Retrieved April 27, 2006.
152. "The History of Electronic Mail". The History of Electronic Mail. Retrieved December 23, 2005.
153. "The First Network Email". The First Network Email. Retrieved December 23, 2005.
154. "Where Have all the Gophers Gone? Why the Web beat Gopher in the Battle for Protocol Mind Share". Ils.unc.edu. Retrieved 2015-10-17.
155. Bush, Vannevar (1945). "As We May Think". Retrieved May 28, 2009.
156. Douglas Engelbart (1962). "Augmenting Human Intellect: A Conceptual Framework".
157. "The Early World Wide Web at SLAC". The Early World Wide Web at SLAC: Documentation of the Early Web at SLAC. Retrieved November 25, 2005.
158. "Millennium Technology Prize 2004 awarded to inventor of World Wide Web". Millennium Technology Prize. Archived from the original on August 30, 2007. Retrieved May 25, 2008.
159. "Mosaic Web Browser History – NCSA, Marc Andreessen, Eric Bina". Livinginternet.com. Retrieved May 28, 2009.
160. "NCSA Mosaic – September 10, 1993 Demo". Totic.org. Retrieved May 28, 2009.
161. "Vice President Al Gore's ENIAC Anniversary Speech". Cs.washington.edu. February 14, 1996. Retrieved May 28, 2009.
162. "UCLA Center for Communication Policy". Digitalcenter.org. Retrieved May 28, 2009.
163. Mirror of Official site map Archived February 21, 2009, at the Wayback Machine.
164. Mirror of Official Site Archived December 22, 2008, at the Wayback Machine.
165. "24 Hours in Cyberspace (and more)". Baychi.org. Retrieved May 28, 2009.
166. "The human face of cyberspace, painted in random images". Archive. southcoasttoday.com. Retrieved May 28, 2009.
167. Stross, Randall (22 September 2009). Planet Google: One Company's Audacious Plan to Organize Everything We Know. Simon and Schuster. ISBN 978-1-4165-4696-2. Retrieved 9 December 2012.
168. "Microsoft's New Search at Bing.com Helps People Make Better Decisions: Decision Engine goes beyond search to help customers deal with information overload (Press Release)". Microsoft News Center. May 28, 2009. Retrieved May 29, 2009.
169. "Microsoft and Yahoo seal web deal", BBC Mobile News, July 29, 2009.
170. RFC 765: File Transfer Protocol (FTP), J. Postel and J. Reynolds, ISI, October 1985
171. Kenneth P. Birman (2005-03-25). Reliable Distributed Systems: Technologies,

Web Services, and Applications. Springer-Verlag New York Incorporated. ISBN 9780387215099. Retrieved 2012-01-20.

172. Menta, Richard (July 20, 2001). "Napster Clones Crush Napster. Take 6 out of the Top 10 Downloads on CNet". MP3 Newswire.
173. Movie File-Sharing Booming: Study, Solutions Research Group, Toronto, 24 January 2006
174. Menta, Richard (December 9, 1999). "RIAA Sues Music Startup Napster for $20 Billion". MP3 Newswire.
175. "EFF: What Peer-to-Peer Developers Need to Know about Copyright Law". W2.eff.org. Retrieved 2012-01-20.
176. Kobie, Nicole (November 26, 2010). "Pirate Bay trio lose appeal against jail sentences". pcpro.co.uk. PCPRO. Retrieved November 26, 2010.
177. "Poll: Young Say File Sharing OK", Bootie Cosgrove-Mather, CBS News, 11 February 2009
178. Green, Stuart P. (29 March 2012). "OP-ED CONTRIBUTOR; When Stealing Isn't Stealing". The New York Times. p. 27.
179. Nasdaq peak of 5,048.62
180. Susmita Dasgupta; Somik V. Lall; David Wheeler (2001). Policy Reform, Economic Growth, and the Digital Divide: An Econometric Analysis. World Bank Publications. pp. 1–3. GGKEY:YLS5GEUEBAR. Retrieved 11 February 2013.
181. Hillebrand, Friedhelm (2002). Hillebrand, Friedhelm, ed. GSM and UMTS, The Creation of Global Mobile Communications. John Wiley & Sons. ISBN 0-470-84322-5.
182. Christoph Classen, Susanne Kinnebrock & Maria Löblich (Eds.): Towards Web History: Sources, Methods, and Challenges in the Digital Age. In Historical Social Research 37 (4): 97–188. 2012.
183. Barras, Colin (August 23, 2007). "An Internet Pioneer Ponders the Next Revolution". Illuminating the net's Dark Ages. Retrieved February 26, 2008.

CHAPTER 3

# Network Packet

## Chapter Contents

- **Introduction**

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, Graphics Interchange Format file, Uniform Resource Locator request, and so forth) is sent from one place to another on the Internet, the Transmission Control Protocol (TCP) layer of TCP/IP divides the file into "chunks" of an efficient size for routing. Each of these packets is separately numbered and includes the Internet address of the destination. The individual packets for a given file may travel different routes through the Internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

## INTRODUCTION

A network packet is a formatted unit of data carried by a packet-switched network. Computer communications links that do not support packets, such as traditional point-to-point telecommunications links, simply transmit data as a bit stream. When data is formatted into packets, packet switching is possible and the bandwidth of the communication medium can be better shared among users than with circuit switching.

A packet consists of control information and user data, which is also known as the payload. Control information provides data for delivering the payload, for example: source

and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers.

## Terminology

In the seven-layer OSI model of computer networking, *packet* strictly refers to a data unit at layer 3, the Network Layer. The correct term for a data unit at Layer 2, the Data Link Layer, is a *frame*, and at Layer 4, the Transport Layer, the correct term is a *segment* or *datagram*. For the case of TCP/IP communication over Ethernet, a TCP segment is carried in one or more IP packets, which are each carried in one or more Ethernet frames.

## Packet Framing

Different communications protocols use different conventions for distinguishing between the elements and for formatting the data. For example, in Point-to-Point Protocol, the packet is formatted in 8-bit bytes, and special characters are used to delimit the different elements. Other protocols like Ethernet, establish the start of the header and data elements by their location relative to the start of the packet. Some protocols format the information at a bit level instead of a byte level.

A good analogy is to consider a packet to be like a letter: the header is like the envelope, and the data area is whatever the person puts inside the envelope.

A network design can achieve two major results by using packets: *error detection* and *multiple host addressing*. A packet has the following components.

### *Addresses*

The routing of network packets requires two network addresses, the source address of the sending host, and the destination address of the receiving host.

### *Error Detection and Correction*

Error detection and correction is performed at various layers in the protocol stack. Network packets may contain a checksum, parity bits or cyclic redundancy checks to detect errors that occur during transmission.

At the transmitter, the calculation is performed before the packet is sent. When received at the destination, the checksum is recalculated, and compared with the one in the packet. If discrepancies are found, the packet may be corrected or discarded. Any packet loss is dealt with by the network protocol.

In some cases modifications of the network packet may be necessary while routing, in which cases checksums are recalculated.

### *Hop Counts*

Under fault conditions packets can end up traversing a closed circuit. If nothing was done, eventually the number of packets circulating would build up until the network was

congested to the point of failure. A time to live is a field that is decreased by one each time a packet goes through a network node. If the field reaches zero, routing has failed, and the packet is discarded.

Ethernet packets have no time-to-live field and so are subject to broadcast radiation in the presence of a switch loop.

### Length

There may be a field to identify the overall packet length. However, in some types of networks, the length is implied by the duration of transmission.

### Priority

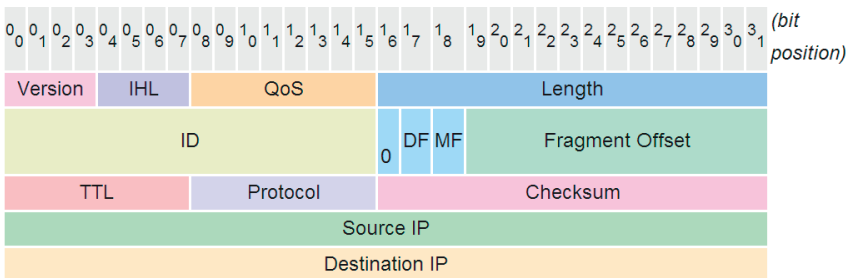
Some networks implement quality of service which can prioritize some types of packets above others. This field indicates which packet queue should be used; a high priority queue is emptied more quickly than lower priority queues at points in the network where congestion is occurring.

### Payload

In general, payload is the data that is carried on behalf of an application. It is usually of variable length, up to a maximum that is set by the network protocol and sometimes the equipment on the route. Some networks can break a larger packet into smaller packets when necessary.

## Example: IP Packets

IP packets are composed of a header and payload. The IPv4 packet header consists of:




- 4 bits that contain the *version*, that specifies if it's an IPv4 or IPv6 packet,
- 4 bits that contain the *Internet Header Length*, which is the length of the header in multiples of 4 bytes (e.g., 5 means 20 bytes).
- 8 bits that contain the *Type of Service*, also referred to as Quality of Service (QoS), which describes what priority the packet should have,
- 16 bits that contain the *length* of the packet in bytes,

- 16 bits that contain an *identification tag* to help reconstruct the packet from several fragments,
- 3 bits. The first contains a zero, followed by a flag that says whether the packet is allowed to be *fragmented* or not (DF: Don't fragment), and a flag to state whether more fragments of a packet follow (MF: More Fragments)
- 13 bits that contain the *fragment offset*, a field to identify position of fragment within original packet
- 8 bits that contain the *Time to live* (TTL), which is the number of hops (router, computer or device along a network) the packet is allowed to pass before it dies (for example, a packet with a TTL of 16 will be allowed to go across 16 routers to get to its destination before it is discarded),
- 8 bits that contain the *protocol* (TCP, UDP, ICMP, etc.)
- 16 bits that contain the *Header Checksum,* a number used in error detection,
- 32 bits that contain the *source IP address*,
- 32 bits that contain the *destination address*.

After those 160 bits, optional flags can be added of varied length, which can change based on the protocol used, then the data that packet carries is added. An IP packet has no trailer. However, an IP packet is often carried as the payload inside an Ethernet frame, which has its own header and trailer.

Many networks do not provide guarantees of delivery, non-duplication of packets, or in-order delivery of packets, e.g., the UDP protocol of the Internet. However, it is possible to layer a transport protocol on top of the packet service that can provide such protection; TCP and UDP are the best examples of layer 4, the Transport Layer, of the seven layered OSI model.

## Example: The NASA Deep Space Network

The Consultative Committee for Space Data Systems (CCSDS) packet telemetry standard defines the protocol used for the transmission of spacecraft instrument data over the deep-space channel. Under this standard, an image or other data sent from a spacecraft instrument is transmitted using one or more packets.

### *CCSDS Packet Definition*

A packet is a block of data with length that can vary between successive packets, ranging from 7 to 65,542 bytes, including the packet header.

- Packetized data is transmitted via frames, which are fixed-length data blocks. The size of a frame, including frame header and control information, can range up to 2048 bytes.
- Packet sizes are fixed during the development phase.

Because packet lengths are variable but frame lengths are fixed, packet boundaries usually do not coincide with frame boundaries.

### Telecom Processing Notes

Data in a frame is typically protected from channel errors by error-correcting codes.

- Even when the channel errors exceed the correction capability of the error-correcting code, the presence of errors is nearly always detected by the error-correcting code or by a separate error-detecting code.
- Frames for which uncorrectable errors are detected are marked as undecodable and typically are deleted.

### Handling Data Loss

Deleted undecodable whole frames are the principal type of data loss that affects compressed data sets. In general, there would be little to gain from attempting to use compressed data from a frame marked as undecodable.

- When errors are present in a frame, the bits of the subband pixels are already decoded before the first bit error will remain intact, but all subsequent decoded bits in the segment usually will be completely corrupted; a single bit error is often just as disruptive as many bit errors.
- Furthermore, compressed data usually are protected by powerful, long-blocklength error-correcting codes, which are the types of codes most likely to yield substantial fractions of bit errors throughout those frames that are undecodable.

Thus, frames with detected errors would be essentially unusable even if they were not deleted by the frame processor.

This data loss can be compensated for with the following mechanisms.

- If an erroneous frame escapes detection, the decompressor will blindly use the frame data as if they were reliable, whereas in the case of detected erroneous frames, the decompressor can base its reconstruction on incomplete, but not misleading, data.
- However, it is extremely rare for an erroneous frame to go undetected.
- For frames coded by the CCSDS Reed–Solomon code, fewer than 1 in 40,000 erroneous frames can escape detection.
- All frames not employing the Reed–Solomon code use a cyclic redundancy check (CRC) error-detecting code, which has an undetected frame-error rate of less than 1 in 32,000.

## Example: Radio and TV Broadcasting

### MPEG Packetized Stream

Packetized Elementary Stream (PES) is a specification defined by the MPEG communication protocol (see the MPEG-2 standard) that allows an elementary stream to be divided into packets. The elementary stream is packetized by encapsulating sequential data bytes from the elementary stream inside PES packet headers.

A typical method of transmitting elementary stream data from a video or audio encoder is to first create PES packets from the elementary stream data and then to encapsulate these PES packets inside an MPEG transport stream (TS) packets or an MPEG program stream (PS). The TS packets can then be multiplexed and transmitted using broadcasting techniques, such as those used in an ATSC and DVB.

## PES Packet Header

| Name | Size | Description |
|---|---|---|
| Packet start code prefix | 3 bytes | 0x000001 |
| Stream id | 1 byte | Examples: Audio streams (0xC0-0xDF), Video streams (0xE0-0xEF) |
| | | Note: The above 4 bytes is called the 32-bit start code. |
| PES Packet length | 2 bytes | Can be zero as in not specified for video streams in MPEG transport streams |
| Optional PES header | variable length | |
| Stuffing bytes | variable length | |
| Data | | See elementary stream. In the case of private streams the first byte of the payload is the sub-stream number. |

Optional PES Header

| Name | Number of Bits | Description |
|---|---|---|
| Marker bits | 2 | **10** binary or 0x2 hex |
| Scrambling control | 2 | 00 implies not scrambled |
| Priority | 1 | |
| Data alignment indicator | 1 | 1 indicates that the PES packet header is immediately followed by the video start code or audio syncword |
| Copyright | 1 | 1 implies copyrighted |
| Original or Copy | 1 | 1 implies original |
| PTS DTS indicator | 2 | 11 = both present, 10 = only PTS |
| ESCR flag | 1 | |
| ES rate flag | 1 | |
| DSM trick mode flag | 1 | |
| Additional copy info flag | 1 | |
| CRC flag | 1 | |
| extension flag | 1 | |
| PES header length | 8 | gives the length of the remainder of the PES header |

| | | |
|---|---|---|
| Optional fields | variable length | presence is determined by flag bits above |
| Stuffing Bytes | variable length | 0xff |

## NICAM

In order to provide mono "compatibility", the NICAM signal is transmitted on a subcarrier alongside the sound carrier. This means that the FM or AM regular mono sound carrier is left alone for reception by monaural receivers.

A NICAM-based stereo-TV infrastructure can transmit a stereo TV programme as well as the mono "compatibility" sound at the same time, or can transmit two or three entirely different sound streams. This latter mode could be used to transmit audio in different languages, in a similar manner to that used for in-flight movies on international flights. In this mode, the user can select which soundtrack to listen to when watching the content by operating a "sound-select" control on the receiver.

NICAM offers the following possibilities. The mode is auto-selected by the inclusion of a 3-bit type field in the data-stream

- One digital stereo sound channel.
- Two completely different digital mono sound channels.
- One digital mono sound channel and a 352 kbit/s data channel.
- One 704 kbit/s data channel.

The four other options could be implemented at a later date. Only the first two of the ones listed are known to be in general use however.

## NICAM Packet Transmission

The NICAM packet (except for the header) is scrambled with a nine-bit pseudo-random bit-generator before transmission.

- The topology of this pseudo-random generator yields a bitstream with a repetition period of 511 bits.
- The pseudo-random generator's polynomial is: **x^9 + x^4 + 1**.
- The pseudo-random generator is initialized with: **111111111**.

Making the NICAM bitstream look more like white noise is important because this reduces signal patterning on adjacent TV channels.

- The NICAM header is not subject to scrambling. This is necessary so as to aid in locking on to the NICAM data stream and resynchronisation of the data stream at the receiver.
- At the start of each NICAM packet the pseudo-random bit generator's shift-register is reset to all-ones.

## REFERENCES

1. "Understanding The OSI Reference Model: An Analogy", The TCP/IP Guide, retrieved 2014-08-09
2. RFC 791
3. Standards" (PDF). DVB. Retrieved 2014-01-23.
4. Method and apparatus for changing codec to reproduce video and/or audio data streams encoded by different codecs within a channel - Patent EP1827030
5. European publication server
6. https://publications.european-patent-office.org/PublicationServer/document.jsp?PN=EP1827030%20EP%201827030&iDocId=6296342&iFormat=0

CHAPTER 4

# Network Topology

## Chapter Contents

- **Introduction**
- **Local Area Network**
- **Metropolitan Area Network**
- **Wide Area Network**

A network topology is the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology.

## INTRODUCTION

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network and may be depicted physically or logically. Physical topology is the placement of the various components of a network, including device location and cable installation, while logical topology illustrates how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical.

An example is a local area network (LAN). Any given node in the LAN has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network. Conversely, mapping the data flow between the components determines the logical topology of the network.

## Topology

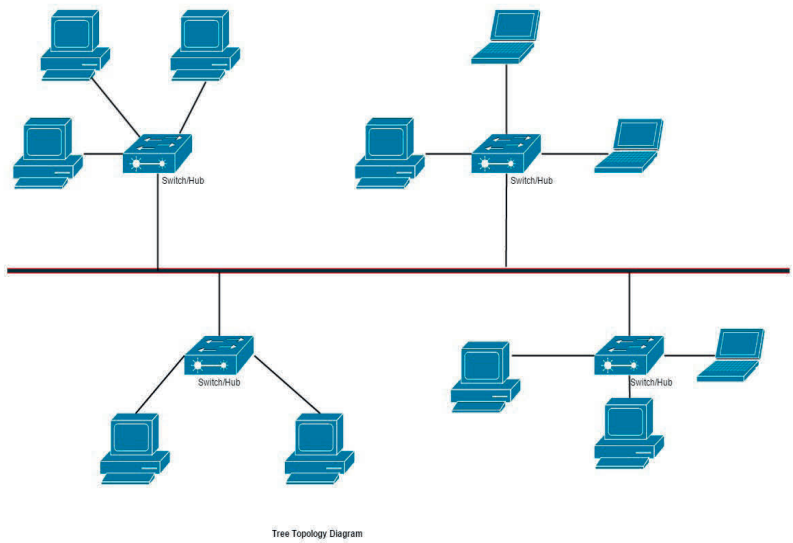



Diagram of different network topologies.

Two basic categories of network topologies exist, physical topologies and logical topologies.

The cabling layout used to link devices is the physical topology of the network. This refers to the layout of cabling, the locations of nodes, and the interconnections between the nodes and the cabling. The physical topology of a network is determined by the capabilities of the network access devices and media, the level of control or fault tolerance desired, and the cost associated with cabling or telecommunications circuits.

In contrast, logical topology is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. A network's logical topology is not necessarily the same as its physical topology. For example, the original twisted pair Ethernet using repeater hubs was a logical bus topology carried on a physical star topology. Token ring is a logical ring topology, but is wired as a physical star from the media access unit. Logical topologies are often closely associated with media access control methods and protocols. Some networks are able to dynamically change their logical topology through configuration changes to their routers and switches.

## Classification

The study of network topology recognizes eight basic topologies: point-to-point, bus, star, ring or circular, mesh, tree, hybrid, or daisy chain.

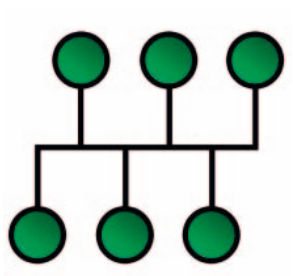
## Point-To-Point

The simplest topology with a dedicated link between two endpoints. Easiest to understand, of the variations of point-to-point topology, is a point-to-point communications channel that appears, to the user, to be permanently associated with the two endpoints. A child's tin can telephone is one example of a *physical dedicated* channel.

Using circuit-switching or packet-switching technologies, a point-to-point circuit can be set up dynamically and dropped when no longer needed. Switched point-to-point topologies are the basic model of conventional telephony.

The value of a permanent point-to-point network is unimpeded communications between the two endpoints. The value of an on-demand point-to-point connection is proportional to the number of potential pairs of subscribers and has been expressed as Metcalfe's Law.

## Bus



Bus network topology

In local area networks where bus topology is used, each node is connected to a single cable, by the help of interface connectors. This central cable is the backbone of the network and is known as the bus (thus the name). A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Because the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, because only one cable is utilized, it can be the single point of failure.

## Linear Bus

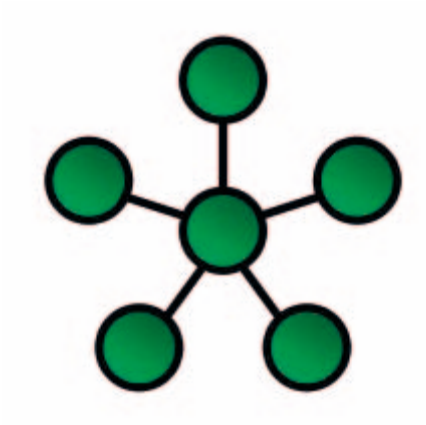
The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

**Note:** When the electrical signal reaches the end of the bus, the signal is reflected back down the line, causing unwanted interference. As a solution, the two endpoints of the bus are normally terminated with a device called a terminator that prevents this reflection.

## Distributed Bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

## Star



Star network topology

In local area networks with a star topology, each network host is connected to a central hub with a point-to-point connection. So it can be said that every computer is indirectly connected to every other node with the help of the hub. In Star topology, every node (computer workstation or any other peripheral) is connected to a central node called hub, router or switch. The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device. All traffic that traverses the network passes through the central hub. The hub acts as a signal repeater. The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the hub represents a single point of failure.

## Extended Star

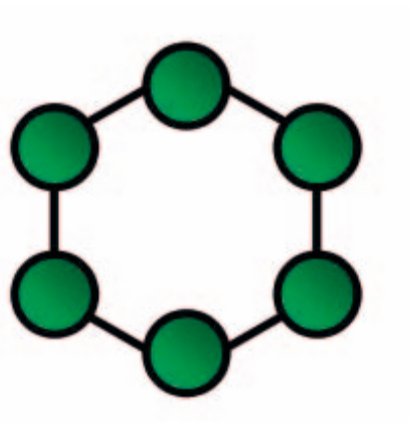
A type of network topology in which a network that is based upon the physical star topology has one or more repeaters between the central node and the peripheral or

'spoke' nodes, the repeaters being used to extend the maximum transmission distance of the point-to-point links between the central node and the peripheral nodes beyond that which is supported by the transmitter power of the central node or beyond that which is supported by the standard upon which the physical layer of the physical star network is based. If the repeaters in a network that is based upon the physical extended star topology are replaced with hubs or switches, then a hybrid network topology is created that is referred to as a physical hierarchical star topology, although some texts make no distinction between the two topologies.

## Distributed Star

A type of network topology that is composed of individual networks that are based upon the physical star topology connected in a linear fashion – i.e., 'daisy-chained' – with no central or top level connection point (e.g., two or more 'stacked' hubs, along with their associated star connected nodes or 'spokes').

## Ring



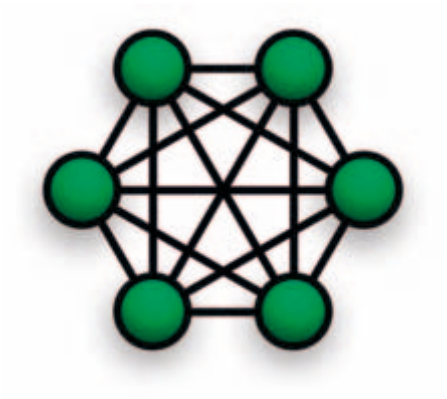
Ring network topology

A ring topology is a bus topology in a closed loop. Data travels around the ring in one direction. When one node sends data to another, the data passes through each intermediate node on the ring until it reaches its destination. The intermediate nodes repeat (retransmit) the data to keep the signal strong. Every node is a peer; there is no hierarchical relationship of clients and servers. If one node is unable to retransmit data, it severs communication between the nodes before and after it in the bus.

## Mesh

The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

## Fully Connected Network



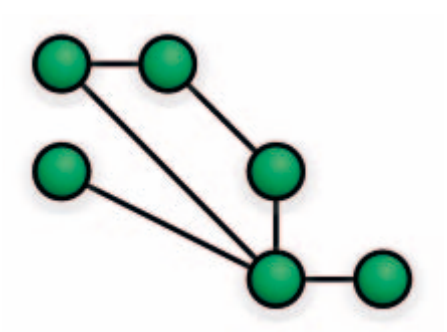
Fully connected mesh topology

In a *fully connected network*, all nodes are interconnected. (In graph theory this is called a complete graph.) The simplest fully connected network is a two-node network. A fully connected network doesn't need to use packet switching or broadcasting. However, since the number of connections grows quadratically with the number of nodes:

$$c = \frac{n(n-1)}{2}.$$

This makes it impractical for large networks.

## Partially Connected Network



Partially connected mesh topology

In a partially connected network, certain nodes are connected to exactly one other node; but some nodes are connected to two or more other nodes with a point-to-point link. This makes it possible to make use of some of the redundancy of mesh topology

that is physically fully connected, without the expense and complexity required for a connection between every node in the network.

### Hybrid

Hybrid networks combine two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example, a tree network (or *star-bus network*) is a hybrid topology in which star networks are interconnected via bus networks. However, a tree network connected to another tree network is still topologically a tree network, not a distinct network type. A hybrid topology is always produced when two different basic network topologies are connected.

A *star-ring* network consists of two or more ring networks connected using a multistation access unit (MAU) as a centralized hub.

Snowflake topology is a star network of star networks.

Two other hybrid network types are *hybrid mesh* and *hierarchical star*.

### Daisy Chain

Except for star-based networks, the easiest way to add more computers into a network is by daisy-chaining, or connecting each computer in series to the next. If a message is intended for a computer partway down the line, each system bounces it along in sequence until it reaches the destination. A daisy-chained network can take two basic forms: linear and ring.

- A linear topology puts a two-way link between one computer and the next. However, this was expensive in the early days of computing, since each computer (except for the ones at each end) required two receivers and two transmitters.
- By connecting the computers at each end, a ring topology can be formed. An advantage of the ring is that the number of transmitters and receivers can be cut in half, since a message will eventually loop all of the way around. When a node sends a message, the message is processed by each computer in the ring. If the ring breaks at a particular link then the transmission can be sent via the reverse path thereby ensuring that all nodes are always connected in the case of a single failure.

## Centralization

The star topology reduces the probability of a network failure by connecting all of the peripheral nodes (computers, etc.) to a central node. When the physical star topology is applied to a logical bus network such as Ethernet, this central node (traditionally a hub) rebroadcasts all transmissions received from any peripheral node to all peripheral nodes on the network, sometimes including the originating node. All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central node

only. The failure of a transmission line linking any peripheral node to the central node will result in the isolation of that peripheral node from all others, but the remaining peripheral nodes will be unaffected. However, the disadvantage is that the failure of the central node will cause the failure of all of the peripheral nodes.

If the central node is *passive*, the originating node must be able to tolerate the reception of an echo of its own transmission, delayed by the two-way round trip transmission time (i.e. to and from the central node) plus any delay generated in the central node. An *active* star network has an active central node that usually has the means to prevent echo-related problems.

A tree topology (a.k.a. hierarchical topology) can be viewed as a collection of star networks arranged in a hierarchy. This tree has individual peripheral nodes (e.g. leaves) which are required to transmit to and receive from one other node only and are not required to act as repeaters or regenerators. Unlike the star network, the functionality of the central node may be distributed.

As in the conventional star network, individual nodes may thus still be isolated from the network by a single-point failure of a transmission path to the node. If a link connecting a leaf fails, that leaf is isolated; if a connection to a non-leaf node fails, an entire section of the network becomes isolated from the rest.

To alleviate the amount of network traffic that comes from broadcasting all signals to all nodes, more advanced central nodes were developed that are able to keep track of the identities of the nodes that are connected to the network. These network switches will "learn" the layout of the network by "listening" on each port during normal data transmission, examining the data packets and recording the address/identifier of each connected node and which port it is connected to in a lookup table held in memory. This lookup table then allows future transmissions to be forwarded to the intended destination only.

## Decentralization

In a partially connected mesh topology, there are at least two nodes with two or more paths between them to provide redundant paths in case the link providing one of the paths fails. Decentralization is often used to compensate for the single-point-failure disadvantage that is present when using a single device as a central node (e.g., in star and tree networks). A special kind of mesh, limiting the number of hops between two nodes, is a hypercube. The number of arbitrary forks in mesh networks makes them more difficult to design and implement, but their decentralized nature makes them very useful. In 2012 the IEEE published the Shortest Path Bridging protocol to ease configuration tasks and allows all paths to be active which increases bandwidth and redundancy between all devices.

This is similar in some ways to a grid network, where a linear or ring topology is used to connect systems in multiple directions. A multidimensional ring has a toroidal topology, for instance.

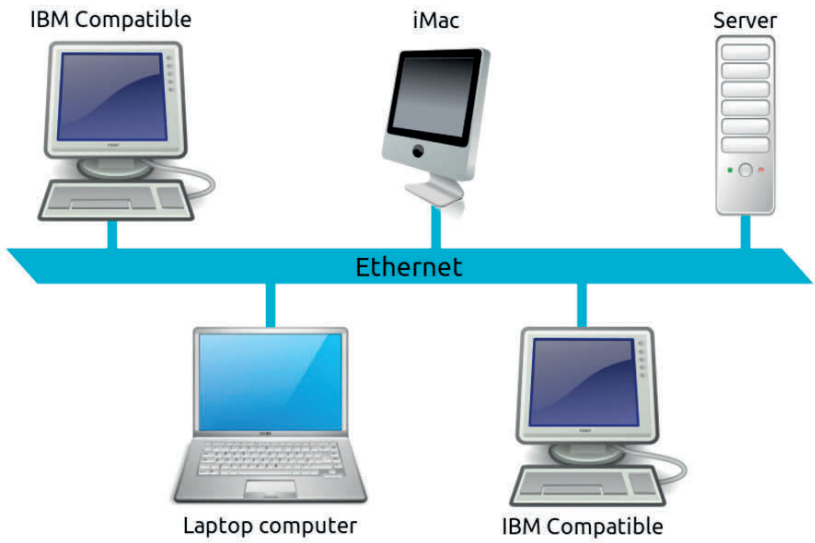
A *fully connected network*, *complete topology*, or *full mesh topology* is a network topology in which there is a direct link between all pairs of nodes. In a fully connected network with n nodes, there are n(n-1)/2 direct links. Networks designed with this topology are usually very expensive to set up, but provide a high degree of reliability due to the

multiple paths for data that are provided by the large number of redundant links between nodes. This topology is mostly seen in military applications.

## LOCAL AREA NETWORK

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building and has its network equipment and interconnects locally managed. By contrast, a wide area network (WAN), not only covers a larger geographic distance, but also generally involves leased telecommunication circuits or Internet links.

Ethernet and Wi-Fi are the two most common transmission technologies in use for local area networks. Historical technologies include ARCNET, Token ring, and AppleTalk.




A conceptual diagram of a local area network using 10BASE5 Ethernet

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

A number of experimental and early commercial LAN technologies were developed in the 1970s. Cambridge Ring was developed at Cambridge University starting in 1974. Ethernet was developed at Xerox PARC in 1973–1975, and filed as U.S. Patent 4,063,220. In 1976, after the system was deployed at PARC, Robert Metcalfe and David Boggs published a seminal paper, "Ethernet: Distributed Packet-Switching for Local Computer Networks". ARCNET was developed by Datapoint Corporation in 1976 and announced in 1977. It had the first commercial installation in December 1977 at Chase Manhattan Bank in New York.

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

In practice, the concept was marred by proliferation of incompatible physical layer and network protocol implementations, and a plethora of methods of sharing resources. Typically, each vendor would have its own type of network card, cabling, protocol, and network operating system. A solution appeared with the advent of Novell NetWare which provided even-handed support for dozens of competing card/cable types, and a much more sophisticated operating system than most of its competitors. Netware dominated the personal computer LAN business from early after its introduction in 1983 until the mid-1990s when Microsoft introduced Windows NT Advanced Server and Windows for Workgroups.

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

During the same period, Unix workstations were using TCP/IP based networking. Although this market segment is now much reduced, the technologies developed in this area continue to be influential on the Internet and in both Linux and Apple Mac OS X networking—and the TCP/IP protocol has now almost completely replaced IPX, AppleTalk, NBF, and other protocols used by the early PC LANs.

## Cabling

Early LAN cabling had generally been based on various grades of coaxial cable. Shielded twisted pair was used in IBM's Token Ring LAN implementation, but in 1984, StarLAN showed the potential of simple *unshielded* twisted pair by using Cat3 cable—the same simple cable used for telephone systems. This led to the development of 10BASE-T (and its successors) and structured cabling which is still the basis of most commercial LANs today. While fiber-optic cabling is common for links between switches, use of fiber to the desktop is rare.

## Wireless Media

Many LANs are now based partly or wholly on wireless technologies. Smartphones, tablet computers and laptops typically have wireless networking support built-in. In a wireless local area network, users may move unrestricted in the coverage area. Wireless networks have become popular in residences and small businesses, because of their ease of installation. Guests are often offered Internet access via a hotspot service.

## Technical Aspects

Network topology describes the layout of interconnections between devices and network segments. At the Data Link Layer and Physical Layer, a wide variety of LAN topologies have been used, including ring, bus, mesh and star, but the most common LAN topology in use today is switched Ethernet. At the higher layers, NetBEUI, IPX/SPX, AppleTalk and others were once common, but the Internet Protocol Suite (TCP/IP) is now the standard.

Simple LANs generally consist of cabling and one or more switches. A switch can be connected to a router, cable modem, or ADSL modem for Internet access. A LAN can include a wide variety of other network devices such as firewalls, load balancers, and sensors; and more complex LANs are characterized by their use of redundant links with switches using the spanning tree protocol to prevent loops, their ability to manage differing traffic types via quality of service (QoS), and to segregate traffic with VLANs.

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

## METROPOLITAN AREA NETWORK

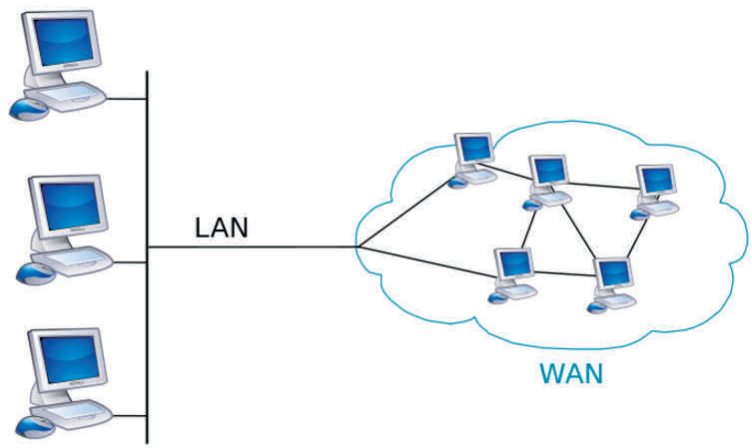
A metropolitan area network (MAN) is a computer network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network. A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN)..

## WIDE AREA NETWORK

A wide area network (WAN) is a telecommunications network or computer network that extends over a large geographical distance. Wide area networks are often established with leased telecommunication circuits.

Business, education and government entities use wide area networks to relay data among staff, students, clients, buyers, and suppliers from various geographical locations. In essence, this mode of telecommunication allows a business to effectively carry out its daily function regardless of location. The Internet may be considered a WAN.

Related terms for other types of networks are personal area networks (PANs), local area networks (LANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area respectively.




## Design Options

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

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

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

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

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

## Connection Technology

Many technologies are available for wide area network links. Examples include circuit switched telephone lines, radio wave transmission, and optic fiber. New developments in technologies have successively increased transmission rates. In ca. 1960, a 110 bit/s (bits per second) line was normal on the edge of the WAN, while core links of 56 kbit/s to 64 kbit/s were considered fast. As of 2014, households are connected to the Internet with ADSL, Cable, Wimax, 4G or fiber at speeds ranging from 1 Mbit/s to 1 Gbit/s and the connections in the core of a WAN can range from 1 Gbit/s to 100 Gbit/s.

List of WAN types

- ATM
- Cable modem
- Dial-up
- DSL
- Frame relay
- ISDN
- Leased line
- SONET
- X.25
- SD-WAN

## Asynchronous Transfer Mode

Asynchronous transfer mode (ATM) is, according to the ATM Forum, "a telecommunications concept defined by ANSI and ITU (formerly CCITT) standards for carriage of a complete range of user traffic, including voice, data, and video signals". ATM was developed to meet the needs of the Broadband Integrated Services Digital Network, as defined in the late 1980s, and designed to unify telecommunication and computer networks. It was designed for a network that must handle both traditional high-throughput data traffic (e.g., file transfers), and real-time, low-latency content such as voice and video. The reference model for ATM approximately maps to the three lowest layers of the ISO-OSI reference model: network layer, data link layer, and physical layer. ATM is a core protocol used over the SONET/SDH backbone of the public switched telephone network (PSTN) and Integrated Services Digital Network (ISDN), but its use is declining in favour of all IP.

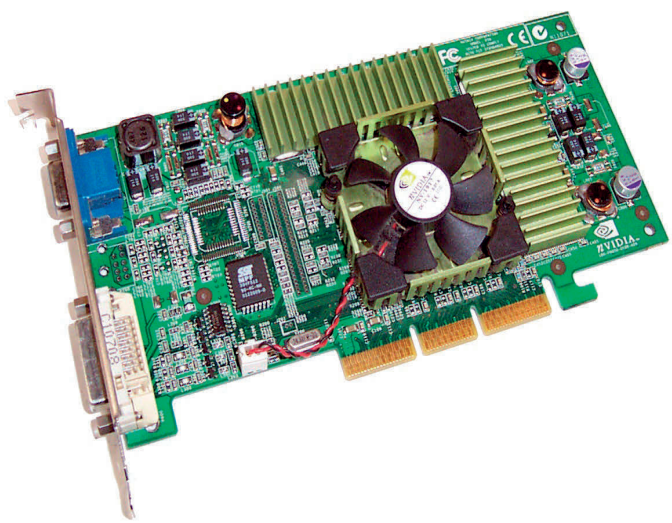
ATM provides functionality that is similar to both circuit switching and packet switching networks: ATM uses asynchronous time-division multiplexing, and encodes data into small, fixed-sized packets (ISO-OSI frames) called cells. This differs from

approaches such as the Internet Protocol or Ethernet that use variable sized packets and frames. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins. These virtual circuits may be "permanent", i.e. dedicated connections that are usually preconfigured by the service provider, or "switched", i.e. set up on a per-call basis using signalling and disconnected when the call is terminated.

ATM eventually became dominated by Internet Protocol (IP) only technology (and Wireless or Mobile ATM never got any foothold).



IBM Turboways ATM 155 PCI network interface card



Marconi ForeRunnerLE 25 ATM PCI network interface card

## Layer 2 – Datagrams

In the ISO-OSI reference model data link layer (layer 2), the basic transfer units are generically called frames. In ATM these frames are of a fixed (53 octets or bytes) length and specifically called "cells".

### *Cell Size*

If a speech signal is reduced to packets, and it is forced to share a link with bursty data traffic (traffic with some large data packets) then no matter how small the speech packets could be made, they would always encounter full-size data packets. Under normal queuing conditions the cells might experience maximum queuing delays. To avoid this issue, all ATM packets, or "cells," are the same small size. In addition, the fixed cell structure means that ATM can be readily switched by hardware without the inherent delays introduced by software switched and routed frames.

Thus, the designers of ATM utilized small data cells to reduce jitter (delay variance, in this case) in the multiplexing of data streams. Reduction of jitter (and also end-to-end round-trip delays) is particularly important when carrying voice traffic, because the conversion of digitized voice into an analogue audio signal is an inherently real-time process, and to do a good job, the decoder (codec) that does this needs an evenly spaced (in time) stream of data items. If the next data item is not available when it is needed, the codec has no choice but to produce silence or guess — and if the data is late, it is useless, because the time period when it should have been converted to a signal has already passed.

At the time of the design of ATM, 155 Mbit/s Synchronous Digital Hierarchy (SDH) with 135 Mbit/s payload was considered a fast optical network link, and many plesiochronous digital hierarchy (PDH) links in the digital network were considerably slower, ranging from 1.544 to 45 Mbit/s in the USA, and 2 to 34 Mbit/s in Europe.

At this rate, a typical full-length 1500 byte (12000-bit) data packet would take 77.42 μs to transmit. In a lower-speed link, such as a 1.544 Mbit/s T1 line, a 1500 byte packet would take up to 7.8 milliseconds.

A queuing delay induced by several such data packets might exceed the figure of 7.8 ms several times over, in addition to any packet generation delay in the shorter speech packet. This was clearly unacceptable for speech traffic, which needs to have low jitter in the data stream being fed into the codec if it is to produce good-quality sound. A packet voice system can produce this low jitter in a number of ways:

- Have a playback buffer between the network and the codec, one large enough to tide the codec over almost all the jitter in the data. This allows smoothing out the jitter, but the delay introduced by passage through the buffer would require echo cancellers even in local networks; this was considered too expensive at the time. Also, it would have increased the delay across the channel, and conversation is difficult over high-delay channels.
- Build a system that can inherently provide low jitter (and minimal overall delay) to traffic that needs it.

- Operate on a 1:1 user basis (i.e., a dedicated pipe).

The design of ATM aimed for a low-jitter network interface. However, "cells" were introduced into the design to provide short queuing delays while continuing to support datagram traffic. ATM broke up all packets, data, and voice streams into 48-byte chunks, adding a 5-byte routing header to each one so that they could be reassembled later. The choice of 48 bytes was political rather than technical. When the CCITT (now ITU-T) was standardizing ATM, parties from the United States wanted a 64-byte payload because this was felt to be a good compromise in larger payloads optimized for data transmission and shorter payloads optimized for real-time applications like voice; parties from Europe wanted 32-byte payloads because the small size (and therefore short transmission times) simplify voice applications with respect to echo cancellation. Most of the European parties eventually came around to the arguments made by the Americans, but France and a few others held out for a shorter cell length. With 32 bytes, France would have been able to implement an ATM-based voice network with calls from one end of France to the other requiring no echo cancellation. 48 bytes (plus 5 header bytes = 53) was chosen as a compromise between the two sides. 5-byte headers were chosen because it was thought that 10% of the payload was the maximum price to pay for routing information. ATM multiplexed these 53-byte cells instead of packets which reduced worst-case cell contention jitter by a factor of almost 30, reducing the need for echo cancellers.

## *The Structure of an ATM Cell*

An ATM cell consists of a 5-byte header and a 48-byte payload. The payload size of 48 bytes was chosen as described above.

ATM defines two different cell formats: UNI (User-Network Interface) and NNI (Network-Network Interface). Most ATM links use UNI cell format.

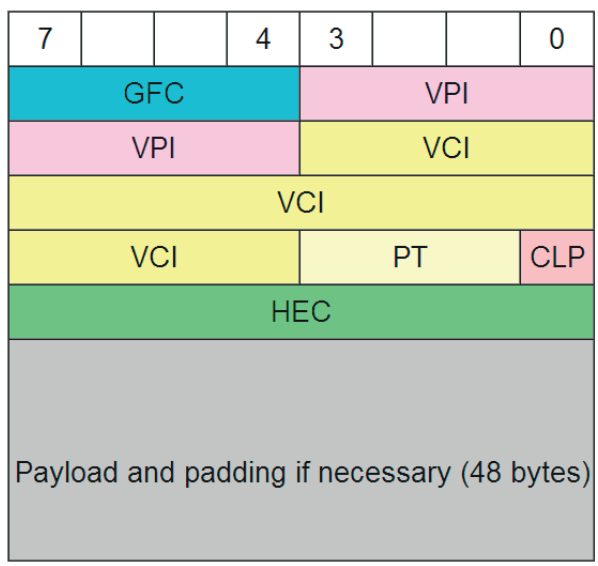



Diagram of the UNI ATM Cell

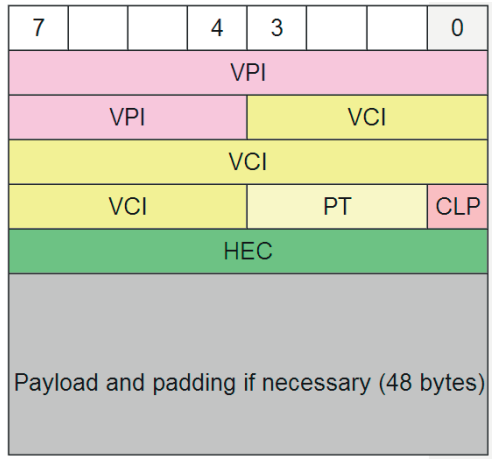



Diagram of the NNI ATM Cell

GFC = Generic Flow Control (4 bits) (default: 4-zero bits)

VPI = Virtual Path Identifier (8 bits UNI, or 12 bits NNI)

VCI = Virtual Channel identifier (16 bits)

PT = Payload Type (3 bits)

PT bit 3 (msbit): Network management cell. If 0, user data cell and the following apply:

PT bit 2: Explicit forward congestion indication (EFCI); 1 = network congestion experienced

PT bit 1 (lsbit): ATM user-to-user (AAU) bit. Used by AAL5 to indicate packet boundaries.

CLP = Cell Loss Priority (1-bit)

HEC = Header Error Control (8-bit CRC, polynomial = $X^8 + X^2 + X + 1$)

ATM uses the PT field to designate various special kinds of cells for operations, administration and management (OAM) purposes, and to delineate packet boundaries in some ATM adaptation layers (AAL). If the most significant bit of the PT field is 0, this is a user data cell, and the other two bits are used to indicate network congestion and as a general purpose header bit available for ATM adaptation layers.

If the msbit of the PT bit is 1, this is a management cell, and the other two bits indicate the type. (Network management segment, network management end-to-end, resource management, and reserved for future use.)

Several ATM link protocols use the HEC field to drive a CRC-based framing algorithm, which allows locating the ATM cells with no overhead beyond what is otherwise needed for header protection. The 8-bit CRC is used to correct single-bit header errors and detect multi-bit header errors. When multi-bit header errors are detected, the current and subsequent cells are dropped until a cell with no header errors is found.

A UNI cell reserves the GFC field for a local flow control/submultiplexing system between users. This was intended to allow several terminals to share a single network

connection, in the same way that two Integrated Services Digital Network (ISDN) phones can share a single basic rate ISDN connection. All four GFC bits must be zero by default.

The NNI cell format replicates the UNI format almost exactly, except that the 4-bit GFC field is re-allocated to the VPI field, extending the VPI to 12 bits. Thus, a single NNI ATM interconnection is capable of addressing almost $2^{12}$ VPs of up to almost $2^{16}$ VCs each (in practice some of the VP and VC numbers are reserved).

## Cells in Practice

ATM supports different types of services via AALs. Standardized AALs include AAL1, AAL2, and AAL5, and the rarely used AAL3 and AAL4. AAL1 is used for constant bit rate (CBR) services and circuit emulation. Synchronization is also maintained at AAL1. AAL2 through AAL4 are used for variable bitrate (VBR) services, and AAL5 for data. Which AAL is in use for a given cell is not encoded in the cell. Instead, it is negotiated by or configured at the endpoints on a per-virtual-connection basis.

Following the initial design of ATM, networks have become much faster. A 1500 byte (12000-bit) full-size Ethernet frame takes only 1.2 µs to transmit on a 10 Gbit/s network, reducing the need for small cells to reduce jitter due to contention. Some consider that this makes a case for replacing ATM with Ethernet in the network backbone. However, it should be noted that the increased link speeds by themselves do not alleviate jitter due to queuing. Additionally, the hardware for implementing the service adaptation for IP packets is expensive at very high speeds. Specifically, at speeds of OC-3 and above, the cost of segmentation and reassembly (SAR) hardware makes ATM less competitive for IP than Packet Over SONET (POS); because of its fixed 48-byte cell payload, ATM is not suitable as a data link layer *directly* underlying IP (without the need for SAR at the data link level) since the OSI layer on which IP operates must provide a maximum transmission unit (MTU) of at least 576 bytes. SAR performance limits mean that the fastest IP router ATM interfaces are STM16 - STM64 which actually compares, while as of 2004 POS can operate at OC-192 (STM64) with higher speeds expected in the future.

On slower or congested links (622 Mbit/s and below), ATM does make sense, and for this reason most asymmetric digital subscriber line (ADSL) systems use ATM as an intermediate layer between the physical link layer and a Layer 2 protocol like PPP or Ethernet.

At these lower speeds, ATM provides a useful ability to carry multiple logical circuits on a single physical or virtual medium, although other techniques exist, such as Multi-link PPP and Ethernet VLANs, which are optional in VDSL implementations. DSL can be used as an access method for an ATM network, allowing a DSL termination point in a telephone central office to connect to many internet service providers across a wide-area ATM network. In the United States, at least, this has allowed DSL providers to provide DSL access to the customers of many internet service providers. Since one DSL termination point can support multiple ISPs, the economic feasibility of DSL is substantially improved.

## Why Virtual Circuits?

ATM operates as a channel-based transport layer, using virtual circuits (VCs). This is encompassed in the concept of the Virtual Paths (VP) and Virtual Channels. Every ATM cell has an 8- or 12-bit Virtual Path Identifier (VPI) and 16-bit Virtual Channel Identifier (VCI) pair defined in its header. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. The length of the VPI varies according to whether the cell is sent on the user-network interface (on the edge of the network), or if it is sent on the network-network interface (inside the network).

As these cells traverse an ATM network, switching takes place by changing the VPI/VCI values (label swapping). Although the VPI/VCI values are not necessarily consistent from one end of the connection to the other, the concept of a circuit *is* consistent (unlike IP, where any given packet could get to its destination by a different route than the others). ATM switches use the VPI/VCI fields to identify the Virtual Channel Link (VCL) of the next network that a cell needs to transit on its way to its final destination. The function of the VCI is similar to that of the data link connection identifier (DLCI) in frame relay and the Logical Channel Number & Logical Channel Group Number in X.25.

Another advantage of the use of virtual circuits comes with the ability to use them as a multiplexing layer, allowing different services (such as voice, Frame Relay, n* 64 channels, IP). The VPI is useful for reducing the switching table of some virtual circuits which have common paths.

## Using Cells and Virtual Circuits for Traffic Engineering

Another key ATM concept involves the traffic contract. When an ATM circuit is set up each switch on the circuit is informed of the traffic class of the connection.

ATM traffic contracts form part of the mechanism by which "quality of service" (QoS) is ensured. There are four basic types (and several variants) which each have a set of parameters describing the connection.

- CBR - Constant bit rate: a Peak Cell Rate (PCR) is specified, which is constant.
- VBR - Variable bit rate: an average or Sustainable Cell Rate (SCR) is specified, which can peak at a certain level, a PCR, for a maximum interval before being problematic.
- ABR - Available bit rate: a minimum guaranteed rate is specified.
- UBR - Unspecified bit rate: traffic is allocated to all remaining transmission capacity.

VBR has real-time and non-real-time variants, and serves for "bursty" traffic. Non-real-time is sometimes abbreviated to vbr-nrt.

Most traffic classes also introduce the concept of Cell Delay Variation Tolerance (CDVT), which defines the "clumping" of cells in time.

## Traffic Policing

To maintain network performance, networks may apply traffic policing to virtual circuits to limit them to their traffic contracts at the entry points to the network, i.e. the user–network interfaces (UNIs) and network-to-network interfaces (NNIs): Usage/Network Parameter Control (UPC and NPC).The reference model given by the ITU-T and ATM Forum for UPC and NPC is the generic cell rate algorithm (GCRA), which is a version of the leaky bucket algorithm. CBR traffic will normally be policed to a PCR and CDVt alone, whereas VBR traffic will normally be policed using a dual leaky bucket controller to a PCR and CDVt and an SCR and Maximum Burst Size (MBS). The MBS will normally be the packet (SAR-SDU) size for the VBR VC in cells.

If the traffic on a virtual circuit is exceeding its traffic contract, as determined by the GCRA, the network can either drop the cells or mark the Cell Loss Priority (CLP) bit (to identify a cell as potentially redundant). Basic policing works on a cell by cell basis, but this is sub-optimal for encapsulated packet traffic (as discarding a single cell will invalidate the whole packet). As a result, schemes such as Partial Packet Discard (PPD) and Early Packet Discard (EPD) have been created that will discard a whole series of cells until the next packet starts. This reduces the number of useless cells in the network, saving bandwidth for full packets. EPD and PPD work with AAL5 connections as they use the end of packet marker: the ATM User-to-ATM User (AUU) Indication bit in the Payload Type field of the header, which is set in the last cell of a SAR-SDU.

## Traffic Shaping

Traffic shaping usually takes place in the network interface card (NIC) in user equipment, and attempts to ensure that the cell flow on a VC will meet its traffic contract, i.e. cells will not be dropped or reduced in priority at the UNI. Since the reference model given for traffic policing in the network is the GCRA, this algorithm is normally used for shaping as well, and single and dual leaky bucket implementations may be used as appropriate.

## Types of Virtual Circuits and Paths

ATM can build virtual circuits and virtual paths either statically or dynamically. Static circuits (permanent virtual circuits or PVCs) or paths (permanent virtual paths or PVPs) require that the circuit is composed of a series of segments, one for each pair of interfaces through which it passes.

PVPs and PVCs, though conceptually simple, require significant effort in large networks. They also do not support the re-routing of service in the event of a failure. Dynamically built PVPs (soft PVPs or SPVPs) and PVCs (soft PVCs or SPVCs), in contrast, are built by specifying the characteristics of the circuit (the service “contract”) and the two end points.

Finally, ATM networks create and remove switched virtual circuits (SVCs) on demand when requested by an end piece of equipment. One application for SVCs is to carry individual telephone calls when a network of telephone switches are inter-connected using ATM. SVCs were also used in attempts to replace local area networks with ATM.

### *Virtual Circuit Routing*

Most ATM networks supporting SPVPs, SPVCs, and SVCs use the Private Network Node Interface or the Private Network-to-Network Interface (PNNI) protocol. PNNI uses the same shortest-path-first algorithm used by OSPF and IS-IS to route IP packets to share topology information between switches and select a route through a network. PNNI also includes a very powerful summarization mechanism to allow construction of very large networks, as well as a call admission control (CAC) algorithm which determines the availability of sufficient bandwidth on a proposed route through a network in order to satisfy the service requirements of a VC or VP.

### *Call Admission and Connection Establishment*

A network must establish a connection before two parties can send cells to each other. In ATM this is called a virtual circuit (VC). It can be a permanent virtual circuit (PVC), which is created administratively on the end points, or a switched virtual circuit (SVC), which is created as needed by the communicating parties. SVC creation is managed by signaling, in which the requesting party indicates the address of the receiving party, the type of service requested, and whatever traffic parameters may be applicable to the selected service. “Call admission” is then performed by the network to confirm that the requested resources are available and that a route exists for the connection.

### *Reference Model*

ATM defines three layers:

- ATM adaptation layer (AAL)
- ATM layer, roughly corresponding to the OSI data link layer
- physical layer, equivalent to the OSI physical layer

## Deployment

ATM became popular with telephone companies and many computer makers in the 1990s. However, even by the end of the decade, the better price/performance of Internet Protocol-based products was competing with ATM technology for integrating real-time and bursty network traffic.Companies such as FORE Systems focused on ATM products, while other large vendors such as Cisco Systems provided ATM as an option.After the burst of the dot-com bubble, some still predicted that “ATM is going to dominate”. However, in 2005 the ATM Forum, which had been the trade organization promoting the technology, merged with groups promoting other technologies, and eventually became the Broadband Forum.

## Wireless ATM or Mobile ATM

Wireless ATM, or Mobile ATM, consists of an ATM core network with a wireless access network. ATM cells are transmitted from base stations to mobile terminals. Mobility

functions are performed at an ATM switch in the core network, known as "crossover switch", which is similar to the MSC (mobile switching center) of GSM Networks. The advantage of Wireless ATM is its high bandwidth and high speed handoffs done at Layer 2. In the early 1990s, Bell Labs and NEC Research Labs worked actively in this field. Andy Hopper from Cambridge University Computer Laboratory also worked in this area. There was a Wireless ATM Forum formed to standardize the technology behind Wireless ATM Networks. The forum was supported by several telecommunication companies, including NEC, Fujitsu, AT&T, etc. Mobile ATM aimed to provide high speed multimedia communications technology, capable of delivering broadband mobile communications beyond that of GSM and WLANs.

## Cable Modem

A cable modem is a type of network bridge and modem that provides bi-directional data communication via radio frequency channels on a hybrid fibre-coaxial (HFC) and radio frequency over glass (RFoG) infrastructure. Cable modems are primarily used to deliver broadband Internet access in the form of cable Internet, taking advantage of the high bandwidth of a HFC and RFoG network. They are commonly deployed in Australia, Europe, Asia and the Americas.




Motorola SURFboard SBV6120E EuroDOCSIS 3.0 cable modem

### *MITRE Cablenet*

Internet Experiment Note (IEN) 96 (1979) describes an early RF cable modem system. From pages 2 and 3 of IEN 96:

The Cable-Bus System

The MITRE/Washington Cablenet system is based on a technology developed at MITRE/Bedford. Similar cable-bus systems are in operation at a number of government sites, e.g. Walter Reed Army Hospital, and the NASA Johnson Space Center, but these are all standalone, local-only networks.

The system uses standard Community Antenna Television (CATV) coaxial cable and microprocessor based Bus Interface Units (BIUs) to connect subscriber computers and terminals to the cable. ... The cable bus consists of two parallel coaxial cables, one inbound and the other outbound. The inbound cable and outbound cable are connected at one end, the headend, and electrically terminated at their other ends. This architecture takes advantage of the well developed unidirectional CATV components. The topology is dendritic (i.e. branched like a tree). ...

The BIUs contain Radio Frequency (RF) modems which modulate a carrier signal to transmit digital information using 1 MHz of the available bandwidth in the 24 MHz frequency range. The remainder of the 294 MHz bandwidth can be used to carry other information channels, such as off-the-air TV, FM, closed circuit TV, or a voice telephone system, or, other digital channels. The data rate of our test-bed system is 307.2 kbps.

### *IEEE 802.3b (10BROAD36)*

The IEEE 802 Committee defined 10BROAD36 in 802.3b-1985 as a 10 Mbps IEEE 802.3/Ethernet broadband system to run up to 3,600 metres (11,800 ft) over CATV coax network cabling. The word *broadband* as used in the original IEEE 802.3 specifications implied operation in frequency-division multiplexed (FDM) channel bands as opposed to digital *baseband* square-waveform modulations (also known as line coding), which begin near zero Hz and theoretically consume infinite frequency bandwidth. (In real-world systems, higher-order signal components become indistinguishable from background noise.) In the market 10BROAD36 equipment was not developed by many vendors nor deployed in many user networks as compared to equipment for IEEE 802.3/Ethernet baseband standards such as 10BASE5 (1983), 10BASE2 (1985), 10BASE-T (1990), etc.

## IEEE 802.7

The IEEE 802 Committee also specified a broadband CATV digital networking standard in 1989 with 802.7-1989. However, like 10BROAD36, 802.7-1989 saw little commercial success.

### *Hybrid Networks*

Hybrid Networks developed, demonstrated and patented the first high-speed, asymmetrical cable modem system in 1990. A key Hybrid Networks insight was that in the nascent days of the Internet, data downloading constitutes the majority of the data traffic, and this can be served adequately with a highly asymmetrical data network (i.e. a large downstream data pipe and many small upstream data pipes). This allowed CATV operators to offer high speed data services immediately without first requiring an expensive system upgrade. Also key was that it saw that the upstream and downstream communications could be on the same or different communications media using different protocols working in each direction to establish a closed loop communications system. The speeds and protocols used in each direction would be very different. The earliest systems used the public switched telephone network (PSTN) for the return path since very few cable systems were bi-

directional. Later systems used CATV for the upstream as well as the downstream path. Hybrid's system architecture is used for most cable modem systems today.

## LANcity

LANcity was an early pioneer in cable modems, developing a proprietary system that was widely deployed in the U.S. LANcity, which was led by the Iranian-American engineer Rouzbeh Yassini, was then acquired by Nortel, which eventually spun the cable modem business off as ARRIS. ARRIS continues to make cable modems and CMTS equipment compliant with the DOCSIS standard.

## Zenith Homeworks

Zenith offered a cable modem technology using its own protocol which it introduced in 1993, being one of the first cable modem providers. The Zenith Cable Modem technology was used by several cable television systems in the United States and other countries, including Cox Communications San Diego, Knology in the Southeast United States, Ameritech's Americast service (later to be sold off to Wide Open West after the SBC / Ameritech merger), and Cogeco in Hamilton Ontario. Zenith Homeworks used BPSK (Bi-Phase Shift Keyed) modulation to achieve 500 Kbit/sec in 600 kHz, or 4 Mbit/sec in 6 MHz.

## Com21

Com21 was another early pioneer in cable modems, and quite successful until proprietary systems were made obsolete by the DOCSIS standardization. The Com21 system used a *ComController* as central bridge in CATV network head-ends, the ComPort cable modem in various models and the NMAPS management system using HP OpenView as platform. Later they also introduced a return path multiplexer to overcome noise problems when combining return path signals from multiple areas. The proprietary protocol was based on Asynchronous Transfer Mode (ATM). The central ComController switch was a modular system offering one downstream channel (transmitter) and one management module. The remaining slots could be used for upstream receivers (2 per card), dual Ethernet 10BaseT and later also Fast-Ethernet and ATM interfaces. The ATM interface became the most popular, as it supported the increasing bandwidth demands and also supported VLANs. Com21 developed a DOCSIS modem, but the company filed for bankruptcy in 2003 and closed. The DOCSIS CMTS assets of COM21 were acquired by ARRIS.

## CDLP

CDLP was a proprietary system manufactured by Motorola. CDLP customer premises equipment (CPE) was capable of both PSTN (telephone network) and radio frequency (cable network) return paths. The PSTN-based service was considered 'one-way cable' and had many of the same drawbacks as satellite Internet service; as a result, it quickly gave way to "two-way cable." Cable modems that used the RF cable network for the return path were considered 'two-way cable', and were better able to compete with the

bi-directional digital subscriber line (DSL) service. The standard is in little use now while new providers use, and existing providers having changed to the DOCSIS standard. The Motorola CDLP proprietary CyberSURFR is an example of a device that was built to the CDLP standard, capable of a peak 10 Mbit/s downstream and 1.532 Mbit/s upstream. CDLP supported a maximum downstream bandwidth of 30 Mbit/s which could be reached by using several cable modems.

The Australian ISP BigPond employed this system when it started cable modem tests in 1996. For a number of years cable Internet access was only available in Sydney, Melbourne and Brisbane via CDLP. This network ran parallel to the newer DOCSIS system for several years. In 2004, the CDLP network was terminated and replaced by DOCSIS.

CDLP has been also rolled out at the French cable operator Numericable before upgrading its IP broadband network using DOCSIS.

### DVB/DAVIC

Digital Video Broadcasting (DVB) and Digital Audio Visual Council (DAVIC) are European-formed organizations that developed some cable modem standards. However, these standards have not been as widely adopted as DOCSIS.

### IEEE 802.14

In the mid-1990s the IEEE 802 committee formed a subcommittee (802.14) to develop a standard for cable modem systems. IEEE 802.14 developed a draft standard, which was ATM-based. However, the 802.14 working group was disbanded when North American multi system operators (MSOs) instead backed the then-fledgling DOCSIS 1.0 specification, which generally used best efforts service and was IP-based (with extension codepoints to support ATM for QoS in the future). MSOs were interested in quickly deploying service to compete for broadband Internet access customers instead of waiting on the slower, iterative, and deliberative processes of standards development committees. Albert A. Azzam was Secretary of the IEEE 802.14 Working Group, and his book, *High-Speed Cable Modems*, describes many of the proposals submitted to 802.14.

### IETF

Although the Internet Engineering Task Force (IETF) generally does not generate complete cable modem standards, the IETF chartered Working Groups (WGs) that produced various standards related to cable modem technologies (including 802.14, DOCSIS, PacketCable, and others). In particular, the IETF WGs on IP over Cable Data Network (IPCDN) and IP over Digital Video Broadcasting (DVB) produced some standards applicable to cable modem systems, primarily in the areas of Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) for cable modems and other networking equipment that operates over CATV networks.

### *DOCSIS*

In the late 1990s, a consortium of US cable operators, known as "MCNS" formed to quickly develop an open and interoperable cable modem specification. The group essentially combined technologies from the two dominant proprietary systems at the time, taking the physical layer from the Motorola CDLP system and the MAC layer from the LANcity system. When the initial specification had been drafted, the MCNS consortium handed over control of it to CableLabs which maintained the specification, promoted it in various standards organizations (notably SCTE and ITU), developed a certification testing program for cable modem equipment, and has since drafted multiple extensions to the original specification.

While deployed DOCSIS RFI 1.0 equipment generally only supports best efforts service, the DOCSIS RFI 1.0 Interim-01 document discussed QoS extensions and mechanisms using IntServ, RSVP, RTP, and Synchronous Transfer Mode (STM) telephony (as opposed to ATM). DOCSIS RFI 1.1 later added more robust and standardized QoS mechanisms to DOCSIS. DOCSIS 2.0 added support for S-CDMA PHY, while DOCSIS 3.0 added IPv6 support and channel bonding to allow a single cable modem to use concurrently more than one upstream channel and more than one downstream channel in parallel.

Virtually all cable modems operating in the field today are compliant with one of the DOCSIS versions. Because of the differences in the European PAL and USA's NTSC systems two main versions of DOCSIS exist, DOCSIS and EuroDOCSIS. The main differences are found in the width of RF-channels: 6 MHz for the USA and 8 MHz for Europe. A third variant of DOCSIS was developed in Japan and has seen limited deployment in that country.

Although interoperability was the whole point of the DOCSIS project, most cable operators only approve a very restricted list of cable modems on their network, identifying the ‹allowed' modems by their brand, models, sometimes firmware version and occasionally going as far as imposing a hardware version of the modem, instead of simply allowing a supported DOCSIS version as it should. From this point of view, the DOCSIS standard has failed to provide the promised practical interoperability for the end user.

## Multimedia Terminal Adapter

With the development of voice over Internet Protocol (VoIP) telephony, analog telephone adapters (ATA) have been incorporated into many cable modems for providing telephone service. An embedded ATA is known as an *embedded multimedia terminal adapter* (E-MTA).

Many cable TV service providers also offer VoIP-based telephone service via the cable infrastructure (PacketCable). High-speed Internet access service subscriber may use VoIP telephony by subscribing to a third-party service, such as Vonage, MagicJack+ and NetTALK.

## Network Architectural Functions

In network topology, a cable modem is a network bridge that conforms to IEEE 802.1D for Ethernet networking (with some modifications). The cable modem bridges Ethernet frames between a customer LAN and the coax network. Technically, it is a

modem because it must modulate data to transmit it over the cable network, and it must demodulate data from the cable network to receive it.

With respect to the OSI model of network design, a cable modem is both Physical Layer (Layer 1) device and a Data Link Layer (Layer 2) forwarder. As an IP addressable network node, cable modems support functionality at other layers.

Layer 1 is implemented in the Ethernet PHY on its LAN interface, and a DOCSIS defined cable-specific PHY on its HFC cable interface. The term *cable modem* refers to this cable-specific PHY. The Network Layer (Layer 3) is implemented as an IP host in that it has its own IP address used by the network operator to maintain the device. In the Transport Layer (Layer 4) the cable modem supports UDP in association with its own IP address, and it supports filtering based on TCP and UDP port numbers to, for example, block forwarding of NetBIOS traffic out of the customer's LAN. In the Application Layer (Layer 7), the cable modem supports certain protocols that are used for management and maintenance, notably Dynamic Host Configuration Protocol (DHCP), SNMP, and TFTP.

Some cable modems may incorporate a router and a DHCP server to provide the LAN with IP network addressing. From a data forwarding and network topology perspective, this router functionality is typically kept distinct from the cable modem functionality (at least logically) even though the two may share a single enclosure and appear as one unit, sometimes called a residential gateway. So, the cable modem function will have its own IP address and MAC address as will the router.

## Cable Modem Flap

Cable modems can have a problem known in industry jargon as "flap" or "flapping". A modem flap is when the connection by the modem to the head-end has been dropped (gone offline) and then comes back online. The time offline or rate of flap is not typically recorded, only the incidence. While this is a common occurrence and usually unnoticed, if a modem's flap is extremely high, these disconnects can cause service to be disrupted. If there are usability problems due to flap the typical cause is a defective modem or very high amounts of traffic on the service provider's network (upstream utilization too high). Types of flap include reinsertions, hits and misses, and power adjustments.

## Dial-Up Internet Access

Dial-up Internet access is a form of Internet access that uses the facilities of the public switched telephone network (PSTN) to establish a connection to an Internet service provider (ISP) by dialing a telephone number on a conventional telephone line. The user's computer or router uses an attached modem to encode and decode information into and from audio frequency signals, respectively.

Dial-up Internet has been around since the 1980s via public providers such as NSFNET-linked universities and was first offered commercially in July 1992 by Sprint. Despite losing ground to broadband since the mid-2000s, dial-up may still be used where other forms are not available or the cost is too high, such as in some rural or remote areas.

## Availability

Dial-up connections to the Internet require no infrastructure other than the telephone network and the modems and servers needed to make and answer the calls. Where telephone access is widely available, dial-up remains useful and it is often the only choice available for rural or remote areas, where broadband installations are not prevalent due to low population density and high infrastructure cost. Dial-up access may also be an alternative for users on limited budgets, as it is offered free by some ISPs, though broadband is increasingly available at lower prices in many countries due to market competition.

Dial-up requires time to establish a telephone connection (up to several seconds, depending on the location) and perform configuration for protocol synchronization before data transfers can take place. In locales with telephone connection charges, each connection incurs an incremental cost. If calls are time-metered, the duration of the connection incurs costs.

Dial-up access is a transient connection, because either the user, ISP or phone company terminates the connection. Internet service providers will often set a limit on connection durations to allow sharing of resources, and will disconnect the user—requiring reconnection and the costs and delays associated with it. Technically inclined users often find a way to disable the auto-disconnect program such that they can remain connected for more days than one.

A 2008 Pew research center study stated that only 10 percent of US adults still used dial-up Internet access. The study found that the most common reason for retaining dial-up access was high broadband prices. Users cited lack of infrastructure as a reason less often than stating that they would never upgrade to broadband. According to the United States Federal Communications Commission (FCC), 6% used dial-up in 2010. By 2013, that number had fallen to 3%.

## Replacement by Broadband

Broadband internet access via cable, digital subscriber line, satellite and FTTx has been replacing dial-up access in many parts of the world. Broadband connections typically offer speeds of 700 kbit/s or higher for two-thirds more than the price of dial-up on average. In addition broadband connections are always on, thus avoiding the need to connect and disconnect at the start and end of each session. Finally, unlike dial-up, broadband does not require exclusive use of a phone line and so one can access the Internet and at the same time make and receive voice phone calls without having a second phone line.

However, many rural areas still remain without high speed Internet despite the eagerness of potential customers. This can be attributed to population, location, or sometimes ISPs' lack of interest due to little chance of profitability and high costs to build the required infrastructure. Some dial-up ISPs have responded to the increased competition by lowering their rates and making dial-up an attractive option for those who merely want email access or basic web browsing.

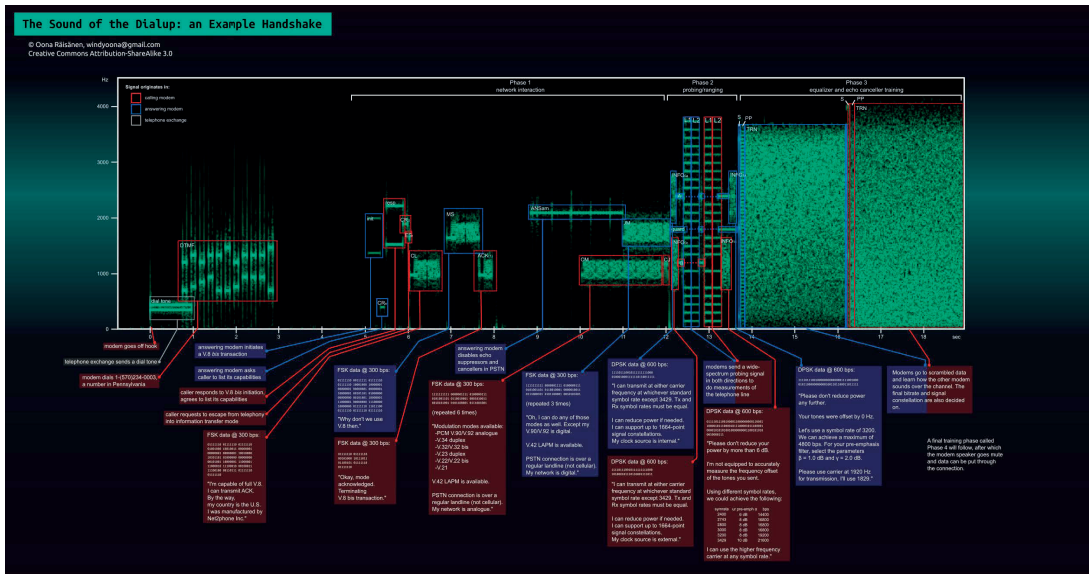
Dial-up Internet access has undergone a precipitous fall in usage, and potentially approaches extinction as modern users turn towards broadband. In contrast to the year 2000

when about 34% of Internet users used dial-up, this dropped to 3% in 2013. Adding to the extinction of dial-up is many newer programs such as antivirus and major applications download their sizable updates automatically in the background when a connection is first made and this can greatly impact the available bandwidth available to other applications like browsers until all updates have completed which may take several minutes or longer. Since an "always on" broadband is the norm expected by most newer applications being developed, this automatic upload trend in the background will continue to eat away at dial-up's available bandwidth to the detriment of dial-up user's applications. Many newer websites also now assume broadband speeds as the norm and when confronted with slower dial-up speeds may drop (timeout) these slower connections to free up communication resources. On websites that are designed to be more dial-up friendly, use of a reverse proxy prevents dial-ups from being dropped as often but can introduce long wait periods for dial-up users caused by the buffering used by a reverse proxy to bridge the different data rates.

## Performance

Modern dial-up modems typically have a maximum theoretical transfer speed of 56 kbit/s (using the V.90 or V.92 protocol), although in most cases, 40–50 kbit/s is the norm. Factors such as phone line noise as well as the quality of the modem itself play a large part in determining connection speeds.

Some connections may be as low as 20 kbit/s in extremely noisy environments, such as in a hotel room where the phone line is shared with many extensions, or in a rural area, many miles from the phone exchange. Other factors such as long loops, loading coils, pair gain, electric fences (usually in rural locations), and digital loop carriers can also slow connections to 20 kbit/s or lower.




An example handshake of a dial-up modem

Analog telephone lines are digitally switched and transported inside a Digital Signal 0 once reaching the telephone company's equipment. Digital Signal 0 is 64 kbit/s; therefore a 56 kbit/s connection is the highest that will ever be possible with analog phone lines.

Dial-up connections usually have latency as high as 150 ms or even more; this is longer than for many forms of broadband, such as cable or DSL, but typically less than satellite connections. Longer latency can make video conferencing and online gaming difficult, if not impossible. An increasing amount of Internet content such as streaming media will not work at dial-up speeds.

Older games released from the mid-1990s to the mid-2000s such as *EverQuest*, *Red Faction*, *Warcraft 3*, *Final Fantasy XI*, *Phantasy Star Online*, *Guild Wars*, *Unreal Tournament*, *Halo: Combat Evolved*, *Audition*, *Quake 3: Arena*, and *Ragnarok Online*, are capable of running on 56k dial-up. The first consoles to provide Internet connectivity, the Dreamcast and PlayStation 2, supported dial-up as well as broadband. The GameCube had an ability to use dial-up and broadband connections, but this was used in very few games and required a separate adapter. The original Xbox exclusively required a broadband connection. Many computer and video games released since the mid-2000s do not even include the option to use dial-up. However, there are exceptions to this, such as *Vendetta Online*, which can still run on a dial-up modem.

## Using Compression to Exceed 56k

The V.42, V.42bis and V.44 standards allow modems to accept uncompressed data at a rate faster than the line rate. These algorithms use data compression to achieve higher throughput.

For instance, a 53.3 kbit/s connection with V.44 can transmit up to 53.3 × 6 = 320 kbit/s if the offered data stream can be compressed that much. However, the compressibility of data tends to vary continuously, for example, due to the transfer of already-compressed files (ZIP files, JPEG images, MP3 audio, MPEG video). A modem might be sending compressed files at approximately 50 kbit/s, uncompressed files at 160 kbit/s, and pure text at 320 kbit/s, or any rate in this range.

## Compression by the ISP

As telephone-based internet lost popularity in the early 2000s, some Internet service providers such as TurboUSA, Netscape, CdotFree, and NetZero started using proxy servers to increase the perceived speed. As an example, EarthLink advertises "surf the Web up to 7x faster" using a compression program that squeezes images, text, and HTML/javascript prior to transmission across the phone line. Citation: http://www.earthlink.net/dialup/

The pre-compression operates much more efficiently than the on-the-fly compression of V.44 modems. Typically website text is compacted to 5% thus increasing effective throughput to approximately 1000 kbit/s, and JPEG/GIF/PNG images are lossy-compressed to 15-20% (increasing throughput up to 300 kbit/s).

The drawback of this approach is a loss in quality, where the graphics acquire compression artifacts taking on a blurry or colorless appearance; however, the

perceived speed is dramatically improved. (If desired the user may choose to view uncompressed images instead.) Also streaming music and video is incompressible, so that kind of data is still limited to 56k, per the limitation of the modem.

## Leased Line

A leased line is a private bidirectional or symmetric telecommunications line between two or more locations provided in exchange for a monthly rent. Sometimes known as a private circuit or data line in the UK.

Unlike traditional PSTN lines it does not have a telephone number, each side of the line being permanently connected to the other. Leased lines can be used for telephone, data or Internet services. Some are ringdown services, and some connect to a Private branch exchange.

Typically, leased lines are used by businesses to connect geographically distant offices. Unlike dial-up connections, a leased line is always active. The fee for the connection is a fixed monthly rate. The primary factors affecting the monthly fee are distance between end points and the speed of the circuit. Because the connection does not carry anybody else's communications, the carrier can assure a given level of quality.

An Internet leased line is a premium internet connectivity product, delivered over fiber normally, which is dedicated and provides uncontended, symmetrical speeds, full-duplex. It is also known as an ethernet leased line, DIA line, data circuit or private circuit.

For example, a T-1 channel can be leased, and provides a maximum transmission speed of 1.544 Mbit/s. The user can divide the connection into different lines for multiplexing data and voice communication, or use the channel for one data circuit. Leased lines, as opposed to DSL, are being used by companies and individuals for Internet access because they afford faster data transfer rates and are cost-effective for heavy users of the Internet.

Leased lines services (or private line services) became digital in the 1970s with the conversion of the Bell backbone network from analog to digital circuits. This allowed AT&T to offer Dataphone Digital Services (later re-branded digital data services) that started the deployment of ISDN and T1 lines to customer premises to connect.

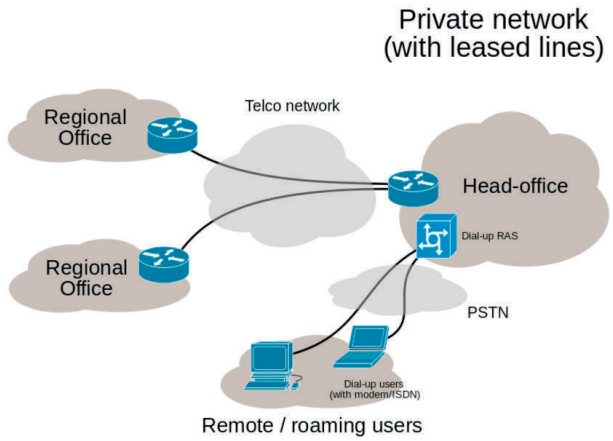
Leased lines were used to connect mainframe computers with terminals and remote sites, via IBM Systems Network Architecture (created in 1974) or DECnet (created in 1975).

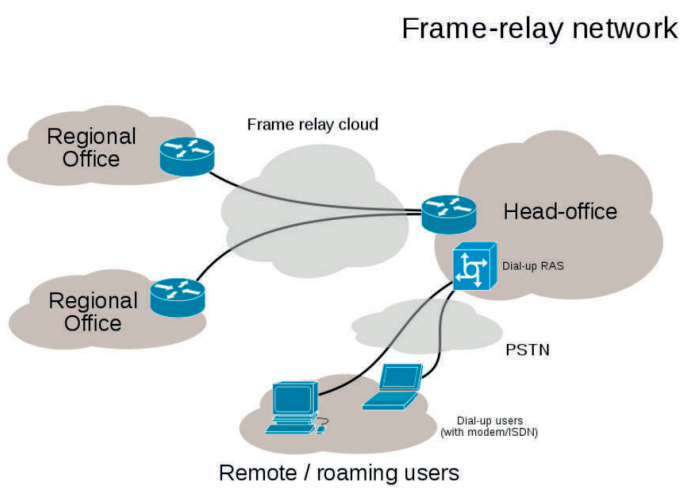
With the extension of digital services in the 1980s leased lines were used to connect customer premises to Frame Relay or ATM networks. Access data rates increased from the original T1 option up to T3 circuits.

In the 1990s with the advances of the Internet, leased lines were also used to connect customer premises to ISP Point of Presence whilst the following decade saw a convergence of the aforementioned services (frame relay, ATM, Internet for businesses) with the MPLS integrated offerings.

Access data rates also evolved dramatically to speeds of up to 10Gbit/s in the early 21st century with the Internet boom and increased offering in long-haul optical networks or Metropolitan Area Networks.

## Applications




Leased lines are used to build up private networks, private telephone networks (by interconnecting PBXs) or access the internet or a partner network (extranet).

Here is a review of the leased line applications in Network designs over time:

### *Site to Site data Connectivity*

Terminating a leased line with two routers can extend network capabilities across sites. Leased lines were first used in the 1970s by enterprise with proprietary protocols such as IBM System Network Architecture and Digital Equipment DECnet, and with TCP/IP in University and Research networks before the Internet became widely available. Note that other Layer 3 protocols were used such as Novell IPX on enterprise networks until TCP/IP became ubiquitous in the 2000s. Today, point to point data circuits are typically provisioned as either TDM, Ethernet, or Layer 3 MPLS.

### Site to Site PBX Connectivity

Terminating a leased line with two PBX allowed customers to by-pass PSTN for inter-site telephony. This allowed the customers to manage their own dial plan (and to use short extensions for internal telephone number) as well as to make significant savings if enough voice traffic was carried across the line (especially when the savings on the telephone bill exceeded the fixed cost of the leased line).

### Site to Network Connectivity

As demand grew on data network telcos started to build more advanced networks using packet switching on top of their infrastructure. Thus, a number of telecommunication companies added ATM, Frame-relay or ISDN offerings to their services portfolio. Leased lines were used to connect the customer site to the telco network access point.

### International Private Leased Circuit

An international private leased circuit (IPLC) functions as a point-to-point private line. IPLCs are usually time-division multiplexing (TDM) circuits that utilize the same circuit amongst many customers. The nature of TDM requires the use of a CSU/DSU and a router. Usually the router will include the CSU/DSU.

Then came the Internet (in the mid-1990s) and since then the most common application for leased line is to connect a customer to its ISP point of presence. With the changes that the Internet brought in the networking world other technologies were developed to propose alternatives to frame-relay or ATM networks such as VPNs (hardware and software) and MPLS networks (that are in effect an upgrade to TCP/IP of existing ATM/frame-relay infrastructures).

## Availability

### In the United Kingdom

In the U.K., leased lines are available at speeds from 64 kbit/s increasing in 64 kbit/s increments to 2.048 Mbit/s over a channelised E1 tail circuit and at speeds between 2.048 Mbit/s to 34.368 Mbit/s via channelised E3 tail circuits. The NTE will terminate the circuit and provide the requested presentation most frequently X.21 however higher speed interfaces are available such as G.703 or 10baseT. Some ISPs however use the term more loosely, defining a leased line as “any dedicated bandwidth service delivered over a leased fibre connection”.

### In the United States

In the U.S., low-speed leased lines (56 kbit/s and below) are usually provided using analog modems. Higher-speed leased lines are usually presented using FT1 (Fractional T1): a T1 bearer circuit with 1 to 24, 56k or 64k timeslots. Customers must manage

their own network termination equipment—Channel Service Unit and Data Service Unit (CSU/DSU).

### *In Hong Kong*

In Hong Kong, leased lines are usually available at speeds of 64k, 128k, 256k, 512k, T1 (channelized or not) or E1 (less common). Whatever the speed, telcos usually provide the CSU/DSU and present to the customer on V.35 interface. Fibre circuits are slowly replacing the traditional circuits and are available at nearly any bandwidth.

### *In India*

In India, leased lines are available at speeds of 64 kbit/s, 128 kbit/s, 256 kbit/s, 512 kbit/s, 1 Mbit/s, 2 Mbit/s, 4 Mbit/s, 8 Mbit/s, 16 Mbit/s T1(1.544 Mbit/s) or E1(2.048 Mbit/s). Customers are connected either through OFC, telephone lines ADSL, or through Wifi. Customers would have to manage their own network termination equipment, namely the Channel service unit and Data service unit.

### *In Italy*

In Italy, leased lines are available at speeds of 64 kbit/s (terminated by DCE2 or DCE2plus modem) or multiple of 64 kbit/s from 128 kbit/s up to framed or unframed E1 (DCE3 modem) in digital form (PDH service, known as CDN, Circuito Diretto Numerico). Local Telephone companies also may provide CDA (Circuito Diretto Analogico), that are plain copper dry pair between two buildings, without any line termination: in the past (pre-2002) a full analog base band was provided, giving an option to customer to deploy xDSL technology between sites: nowadays everything is limited at 4 kHz of bearer channel, so the service is just a POTS connection without any setup channel.

For many purposes, leased lines are gradually being replaced by DSL and metro Ethernet.

## Leased Line Alternatives

Leased lines are more expensive than alternative connectivity services including (ADSL, SDSL, etc.) because they are reserved exclusively to the leaseholder. Some internet service providers have therefore developed alternative products that aim to deliver leased-line type services (Carrier Ethernet-based, zero contention, guaranteed availability), with more moderate bandwidth, over the standard UK national broadband network. While a leased line is full-duplex, most leased line alternatives provide only half-duplex or in many cases asymmetrical service.

## Software-Defined Networking

Software-defined networking (SDN) is an approach to computer networking that allows network administrators to manage network services through abstraction of lower-level

functionality. SDN is meant to address the fact that the static architecture of traditional networks doesn't support the dynamic, scalable computing and storage needs of more modern computing environments such as data centers. This is done by decoupling or disassociating the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane).

SDN was commonly associated with the OpenFlow protocol (for remote communication with network plane elements for the purpose of determining the path of network packets across network switches) since the latter's emergence in 2011. Since 2012, however, many companies have moved away from OpenFlow, and have embraced different techniques. These include Cisco Systems' Open Network Environment and Nicira's network virtualization platform.

SD-WAN applies similar technology to a wide area network (WAN).

The origins of software-defined networking began shortly after Sun Microsystems released Java in 1995.

One of the first SDN projects was AT&T's GeoPlex. AT&T Labs Geoplex project members Michah Lerner, George Vanecek, Nino Vidovic, and Dado Vrsalovic leveraged the network APIs and dynamic aspects of the Java language as a means to implement middleware networks. "GeoPlex is not an operating system, nor does it attempt to compete with one. It is networking middleware that uses one or more operating systems running on computers, connected to the Internet. GeoPlex is a service platform that manages networks and on-line services. GeoPlex maps all of the IP network activities into one or more services."

GeoPlex did not concern itself with operating systems running on networking hardware switches, and routers. AT&T wanted a "soft switch" that could reconfigure physical switches in the network and load them with new services from an operations support system (OSS). However, when provisioning services GeoPlex could not reach deeply into the physical devices to perform reconfiguration. The operating systems running on networked devices in the physical network therefore became a barrier to early SDN-like service delivery.

In 1998, Mark Medovich, a senior scientist of Sun Microsystems and Javasoft, left Sun to launch a Silicon Valley soft switch startup WebSprocket. Medovich designed a new network operating system, and an object oriented structured runtime model that could be modified by a networked compiler and class loader in real time. With this approach, applications could be written with Java threads that inherited WebSprocket kernel, network, and device classes and later modified by the networked compiler/class-loader. WebSprocket's platform was designed such that devices had the ability to instantiate network stack(s), interfaces, and protocols as multiple threads.

In July 2000, WebSprocket released VMFoundry, the Java to bare metal structured runtime compiler, and VMServer, a networked device compiler/classloader application server. Custom networked devices were preloaded with images created by VMFoundry then deployed on the network and connected to VMServer via UDP or TCP services plane, which could proactively or reactively load or extend network protocol methods and classes on the target system. WebSprocket's version of SDN, therefore was not

confined to a set of limited actions managed by an SDN controller. Rather, WebSprocket's "control plane" contained code that could change, override, extend, or enhance Network protocols on operating networked systems. Bill Yount (Stanford University Network) visited WebSprocket's Sunnyvale lab to see a demonstration and expressed great enthusiasm about the entire concept, especially the VMServer (SDN Controller) and prophetically stated SDN (WebSprocket) as "10 years ahead of its time". In Summer of 2000, Ericsson's advanced network research engineers saw an immediate need and visited WebSprocket to design and architect features of a next generation soft switch thus taking first steps to build the world's first commercial soft switch.

Sometime during 2000, the Gartner Group introduced the "Supranet", the fusion of the physical and the digital (virtual) worlds as "internet of things," and by October 2000 the Gartner Group selected WebSprocket as one of the top emerging technologies.

In early 2001, Ericsson and WebSprocket entered into a license contract to create the first commercial soft switch. An international consortium was formed to develop standards for the "Supranet". In March 2001, Kurt Dewitt, Supranet Consortium Chairman and Business Development Director for Ericsson's Data Broadband and Optical Networks Division, announced the selection of WebSprocket as the enabling technology of the Supranet Transaction Server (STS), a comprehensive framework to deliver any networked service.

In April and May 2001, Ohio State University and OARnet, collaboratively ran the first SDN test and developed the first practical SDN use case for Internet2. After successful completion of tests, OARnet issued the following statement on May 8, 2001:

"We have witnessed the successful first step to the fulfillment of smart, interoperable networks through the deployment of Supranet Transaction Server. A technology first was accomplished as a new set of instructions was dynamically transmitted across the network, changing the behavior of the requesting computer. There was no need to take down any part of the system and there was no interruption of service. Our testing will continue and we anticipate further advancement of the next generation Internet through our partnership with Websprocket" – Pankaj Shah (Managing Director, OARnet)

The telecom market deflated in 2001 and Ericsson's soft switch development program came to an end, thus stalling the only known commercial SDN soft switch R&D effort at that time.

Software-defined networking was continued with work done in 2003 by Bob Burke and Zac Carman developing the Content Delivery Control Network patent application that eventually was issued as two US patents: 8,122,128 and 8,799,468. In this seminal inception, SDN, named service preference architecture (SPA) in their patent, was described as a collection of network embedded computing techniques used to control the operation of Network Elements, namely content servers, routers, switches and gateways, with the objective being to safeguard content from theft (P2P) or unwanted interception and to efficiently deliver content for paid services. CableLabs later specified Digital Cable and CableCARD using what we now know as SDN, which debuted in 2007. SDN was again moved ahead in work done at UC Berkeley and Stanford University around 2008.

The Open Networking Foundation was founded in 2011 to promote SDN and OpenFlow.

At the 2014 Interop and Tech Field Day, software-defined networking was demonstrated by Avaya using shortest path bridging and OpenStack as an automated campus, extending

automation from the data center to the end device, removing manual provisioning from service delivery.

By 2016, some in the industry thought that SDN had become a meaningless marketing term.

## Concept

Software-defined networking (SDN) is an architecture purporting to be dynamic, manageable, cost-effective, and adaptable, seeking to be suitable for the high-bandwidth, dynamic nature of today's applications. SDN architectures decouple network control and forwarding functions, enabling network control to become directly programmable and the underlying infrastructure to be abstracted from applications and network services.

The OpenFlow protocol can be used in SDN technologies. The SDN architecture is:

- *Directly programmable*: Network control is directly programmable because it is decoupled from forwarding functions.
- *Agile*: Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.
- *Centrally managed*: Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch.
- *Programmatically configured*: SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.
- *Open standards-based and vendor-neutral*: When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.

## The Need for a New Network Architecture

The explosion of mobile devices and content, server virtualization, and advent of cloud services are among the trends driving the networking industry to re-examine traditional network architectures. Many conventional networks are hierarchical, built with tiers of Ethernet switches arranged in a tree structure. This design made sense when client-server computing was dominant, but such a static architecture is ill-suited to the dynamic computing and storage needs of today's enterprise data centers, campuses, and carrier environments. Some of the key computing trends driving the need for a new network paradigm include:

### *Changing Traffic Patterns*

Within the enterprise data center, traffic patterns have changed significantly. In contrast to client-server applications where the bulk of the communication occurs between one

client and one server, today's applications access different databases and servers, creating a flurry of "east-west" machine-to-machine traffic before returning data to the end user device in the classic "north-south" traffic pattern. At the same time, users are changing network traffic patterns as they push for access to corporate content and applications from any type of device (including their own), connecting from anywhere, at any time. Finally, many enterprise data centers managers are contemplating a utility computing model, which might include a private cloud, public cloud, or some mix of both, resulting in additional traffic across the wide area network.

## The "Consumerization of IT"

Users are increasingly employing mobile personal devices such as smartphones, tablets, and notebooks to access the corporate network. IT is under pressure to accommodate these personal devices in a fine-grained manner while protecting corporate data and intellectual property and meeting compliance mandates.

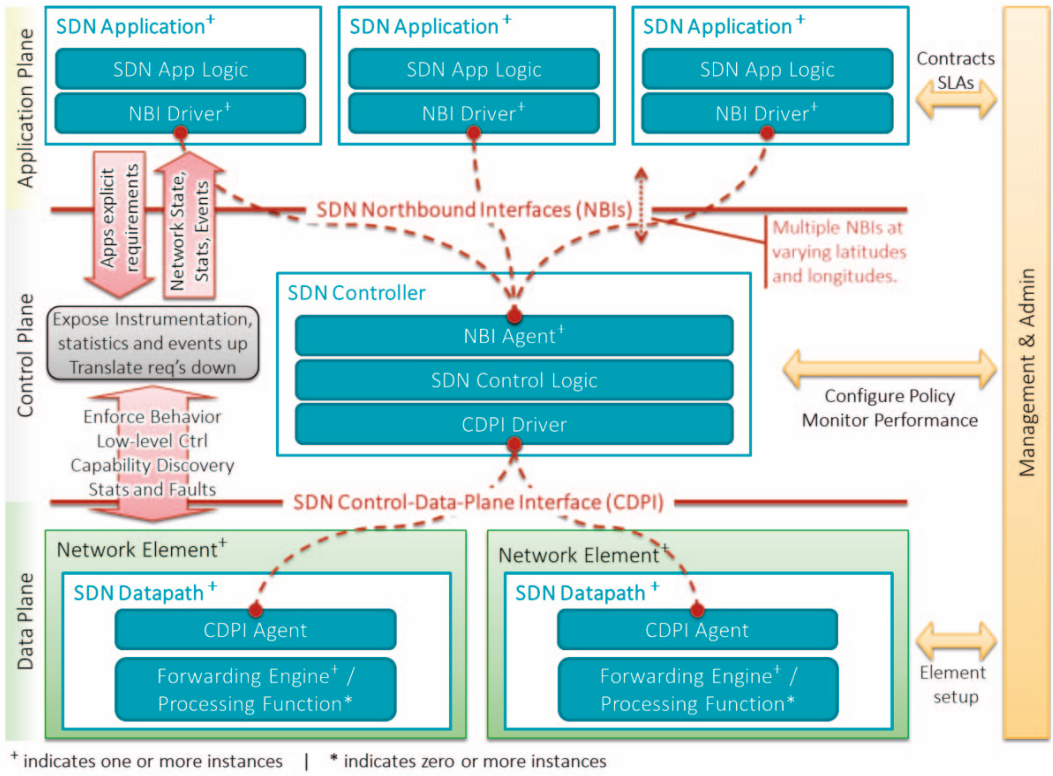
## The Rise of Cloud Services

Enterprises have enthusiastically embraced both public and private cloud services, resulting in unprecedented growth of these services. Enterprise business units now want the agility to access applications, infrastructure, and other IT resources on demand and à la carte. To add to the complexity, IT's planning for cloud services must be done in an environment of increased security, compliance, and auditing requirements, along with business reorganizations, consolidations, and mergers that can change assumptions overnight. Providing self-service provisioning, whether in a private or public cloud, requires elastic scaling of computing, storage, and network resources, ideally from a common viewpoint and with a common suite of tools.

## "Big data" Means more bandwidth

Handling today's "big data" or mega datasets requires massive parallel processing on thousands of servers, all of which need direct connections to each other. The rise of mega datasets is fueling a constant demand for additional network capacity in the data center. Operators of hyperscale data center networks face the daunting task of scaling the network to previously unimaginable size, maintaining any-to-any connectivity without going broke.

## Architectural Components




A high-level overview of the software-defined networking architecture

The following list defines and explains the architectural components:

### *SDN Application*

SDN Applications are programs that explicitly, directly, and programmatically communicate their network requirements and desired network behavior to the SDN Controller via a northbound interface (NBI). In addition they may consume an abstracted view of the network for their internal decision making purposes. An SDN Application consists of one SDN Application Logic and one or more NBI Drivers. SDN Applications may themselves expose another layer of abstracted network control, thus offering one or more higher-level NBIs through respective NBI agents.

### *SDN Controller*

The SDN Controller is a logically centralized entity in charge of (i) translating the requirements from the SDN Application layer down to the SDN Datapaths and (ii) providing the SDN Applications with an abstract view of the network (which may include statistics and events). An SDN Controller consists of one or more NBI Agents, the SDN Control

Logic, and the Control to Data-Plane Interface (CDPI) driver. Definition as a logically centralized entity neither prescribes nor precludes implementation details such as the federation of multiple controllers, the hierarchical connection of controllers, communication interfaces between controllers, nor virtualization or slicing of network resources.

### *SDN Datapath*

The SDN Datapath is a logical network device that exposes visibility and uncontested control over its advertised forwarding and data processing capabilities. The logical representation may encompass all or a subset of the physical substrate resources. An SDN Datapath comprises a CDPI agent and a set of one or more traffic forwarding engines and zero or more traffic processing functions. These engines and functions may include simple forwarding between the datapath's external interfaces or internal traffic processing or termination functions. One or more SDN Datapaths may be contained in a single (physical) network element—an integrated physical combination of communications resources, managed as a unit. An SDN Datapath may also be defined across multiple physical network elements. This logical definition neither prescribes nor precludes implementation details such as the logical to physical mapping, management of shared physical resources, virtualization or slicing of the SDN Datapath, interoperability with non-SDN networking, nor the data processing functionality, which can include OSI layer 4-7 functions.

### *SDN Control to Data-Plane Interface (CDPI)*

The SDN CDPI is the interface defined between an SDN Controller and an SDN Datapath, which provides at least (i) programmatic control of all forwarding operations, (ii) capabilities advertisement, (iii) statistics reporting, and (iv) event notification. One value of SDN lies in the expectation that the CDPI is implemented in an open, vendor-neutral and interoperable way.

### *SDN Northbound Interfaces (NBI)*

SDN NBIs are interfaces between SDN Applications and SDN Controllers and typically provide abstract network views and enable direct expression of network behavior and requirements. This may occur at any level of abstraction (latitude) and across different sets of functionality (longitude). One value of SDN lies in the expectation that these interfaces are implemented in an open, vendor-neutral and interoperable way.

## SDN Control Plane

### *Centralized - Hierarchical - Distributed*

The implementation of the SDN control plane can follow a centralized, hierarchical, or decentralized design. Initial SDN control plane proposals focused on a centralized solution, where a single control entity has a global view of the network. While this simplifies the implementation of the control logic, it has scalability limitations as the size and dynamics

of the network increase. To overcome these limitations, several approaches have been proposed in the literature that fall into two categories, hierarchical and fully distributed approaches. In hierarchical solutions,distributed controllers operate on a partitioned network view, while decisions that require network-wide knowledge are taken by a logically centralized root controller. In distributed approaches, controllers operate on their local view or they may exchange synchronization messages to enhance their knowledge. Distributed solutions are more suitable for supporting adaptive SDN applications.

### *Controller Placement*

A key issue when designing a distributed SDN control plane is to decide on the number and placement of control entities. An important parameter to consider while doing so is the propagation delay between the controllers and the network devices, especially in the context of large networks. Other objectives that have been considered involve control path reliability, fault tolerance, and application requirements.

## Sdn Flow Forwarding (SDN)

### *Proactive Vs Reactive Vs Hybrid*

OpenFlow uses TCAM tables to route packet sequences (flows). If flows arrive at a switch, a flow table lookup is performed. Depending on the flow table implementation this is done in a software flow table if a vSwitch is used or in an ASIC if it's implemented in hardware. In the case when no matching flow is found a request to the controller for further instructions is sent. This is handled in one of three different modes. In reactive mode the controller acts after these requests and creates and installs a rule in the flow table for the corresponding packet if necessary. In proactive mode the controller populates flow table entries for all possible traffic matches possible for this switch in advance. This mode can be compared with typical routing table entries today, where all static entries are installed ahead of time. Following this no request is sent to the controller since all incoming flows will find a matching entry. A major advantage in proactive mode is that all packets are forwarded in line rate (considering all flow table entries in TCAM) and no delay is added. The third mode, hybrid mode, follows the flexibility of a reactive mode for a set of traffic and the low-latency forwarding (proactive mode) for the rest of the traffic.

## Applications

### *SDMN*

**Software-defined mobile networking** (**SDMN**) is an approach to the design of mobile networks where all protocol-specific features are implemented in software, maximizing the use of generic and commodity hardware and software in both the core network and radio

access network. It is proposed as an extension of SDN paradigm to incorporate mobile network specific functionalities.

## SD-WAN

An SD-WAN is a Wide Area Network (WAN) managed using the principles of software-defined networking. The main driver of SD-WAN is to lower WAN costs using less expensive leased lines, as an alternative or partial replacement of more expensive MPLS lines. Control and management is separated from the hardware, with central controllers allowing easier configuration and administration.

## SD-LAN

A SD-LAN is a Local area network (LAN) built around the principles of software-defined networking, though there are key differences in topology, network security, application visibility and control, management and quality of service. SD-LAN decouples control management, and data planes to enable a policy driven architecture for wired and wireless LANs. SD-LANs are characterized by their use of a cloud management system and wireless connectivity without the presence of a physical controller.

## Security Using the SDN Paradigm

SDN architecture may enable, facilitate or enhance network-related security applications due to the controller's central view of the network, and its capacity to reprogram the data plane at any time. While security of SDN architecture itself remains an open question that has already been studied a couple of times in the research community, the following paragraphs only focus on the security applications made possible or revisited using SDN.

Several research works on SDN have already investigated security applications built upon the SDN controller, with different aims in mind. Distributed Denial of Service (DDoS) detection and mitigation, as well as botnet and worm propagation, are some concrete use-cases of such applications: basically, the idea consists in periodically collecting network statistics from the forwarding plane of the network in a standardized manner (e.g. using Openflow), and then apply classification algorithms on those statistics in order to detect any network anomalies. If an anomaly is detected, the application instructs the controller how to reprogram the data plane in order to mitigate it.

Another kind of security application leverages the SDN controller by implementing some moving target defense (MTD) algorithms. MTD algorithms are typically used to make any attack on a given system or network more difficult than usual by periodically hiding or changing key properties of that system or network. In traditional networks, implementing MTD algorithms is not a trivial task since it is difficult to build a central authority able of determining - for each part of the system to be protected - which key properties are hid or changed. In an SDN network, such tasks become more straightforward thanks to the centrality of the controller. One application can for example periodically assign virtual IPs to hosts within the network, and the mapping virtual IP/real IP is then performed by the controller. Another application can simulate some fake opened/closed/

filtered ports on random hosts in the network in order to add significant noise during reconnaissance phase (e.g. scanning) performed by an attacker.

Additional value regarding security in SDN enabled networks can also be gained using FlowVisor and FlowChecker respectively. The former tries to use a single hardware forwarding plane sharing multiple separated logical networks. Following this approach the same hardware resources can be used for production and development purposes as well as separating monitoring, configuration and internet traffic, where each scenario can have its own logical topology which is called slice. In conjunction with this approach FlowChecker realizes the validation of new OpenFlow rules that are deployed by users using their own slice.

SDN controller applications are mostly deployed in large-scale scenarios, which requires comprehensive checks of possible programming errors. A system to do this called NICE was described in 2012. Introducing an overarching security architecture requires a comprehensive and protracted approach to SDN. Since it was introduced, designers are looking at possible ways to secure SDN that do not compromise scalability. One architecture called SN-SECA (SDN+NFV) Security Architecture.

## REFERENCES


1. Groth, David; Toby Skandier (2005). Network+ Study Guide, Fourth Edition. Sybex, Inc. ISBN 0-7821-4406-3.
2. ATIS committee PRQC. “mesh topology”. ATIS Telecom Glossary 2007. Alliance for Telecommunications Industry Solutions. Retrieved 2008-10-10.
3. Chiang, Mung; Yang, Michael (2004). “Towards Network X-ities From a Topological Point of View: Evolvability and Scalability” (PDF). Proc. 42nd Allerton Conference.
4. Inc, S., (2002) . Networking Complete. Third Edition. San Francisco: Sybex
5. Bicsi, B. (2002). Network Design Basics for Cabling Professionals. McGraw-Hill Professional. ISBN 9780071782968.
6. Sosinsky, Barrie A. (2009). “Network Basics”. Networking Bible. Indianapolis: Wiley Publishing. p. 16. ISBN 978-0-470-43131-3. OCLC 359673774. Retrieved 2016-03-26.
7. Bradley, Ray. Understanding Computer Science (for Advanced Level): The Study Guide. Cheltenham: Nelson Thornes. p. 244. ISBN 978-0-7487-6147-0. OCLC 47869750. Retrieved 2016-03-26.
8. “Avaya Extends the Automated Campus to End the Network Waiting Game”. Avaya. 1 April 2014. Retrieved 18 April 2014.
9. Peter Ashwood-Smith (24 February 2011). “Shortest Path Bridging IEEE 802.1aq Overview” (PDF). Huawei. Retrieved 11 May 2012.
10. Jim Duffy (11 May 2012). “Largest Illinois healthcare system uproots Cisco to build $40M private cloud”. PC Advisor. Retrieved 11 May 2012. Shortest Path Bridging will replace Spanning Tree in the Ethernet fabric.

11. "IEEE Approves New IEEE 802.1aq Shortest Path Bridging Standard". Tech Power Up. 7 May 2012. Retrieved 11 May 2012.
12. D. Fedyk, Ed.,; P. Ashwood-Smith, Ed.,; D. Allan, A. Bragg,; P. Unbehagen (April 2012). "IS-IS Extensions Supporting IEEE 802.1aq". IETF. Retrieved 12 May 2012.
13. "Predicting SD-WAN Adoption". gartner.com. 2015-12-15. Retrieved 2016-06-27.
14. "The History of Java Technology". Retrieved October 6, 2012.
15. Sun Pegs Telecom with JTONE
16. Sun facilitates Java use for public network operators
17. "CERIAS : GeoPlex: Universal Service Platform for IP Network-based Services - 10/17/1997". Cerias.purdue.edu. Retrieved 26 October 2014.
18. "Middleware Networks". Dl.acm.org. Retrieved 26 October 2014.
19. "Design Automation of Supranet Systems: Benefits for Hardware Design and Bringup" (PDF). S3us-west-2.amazonaws.com. Retrieved 22 November 2014.
20. "Websprocket Announces VMServer - World's First Proxy Java Virtual Machine; Enables 1,000's of Connected Clients To Use Single Java Virtual Machine.". Thefreelibrary.com. Retrieved 26 October 2014.
21. "Installation Guide". Web.archive.org. Archived from the original on February 4, 2002. Retrieved 22 November 2014.
22. "Top Emerging Technologies Announced During Gartner Symposium/ITxpo 2000; New Emerging Technologies Research Highlights Trends in Wearable Computing, Profiling and Privacy.". Thefreelibrary.com. Retrieved 26 October 2014.
23. "Websprocket Selected By Supranet Consortium to Enable the Internet With Smart Packet Technology; Platform Unifies Supranet Management Through Java and Oracle.". Thefreelibrary.com. Retrieved 26 October 2014.
24. "Software Defined Network SDN". Scribd.com. Retrieved 26 October 2014.
25. "United States Patent: 8122128". Patft.uspto.gov. Retrieved 26 October 2014.
26. "United States Patent: 8799468". Patft.uspto.gov. Retrieved 26 October 2014.
27. "Prof. Scott Shenker - Gentle Introduction to Software-Defined Networking - Technion lecture". YouTube. 2012-06-26. Retrieved 2014-01-23.
28. "Interop 2014: Avaya to showcase Automated Campus part of SDN initiative". Info Tech Lead. 26 March 2014. Retrieved 25 June 2014.
29. "Avaya Software Defined Data Center". Tech Field Day. Feb 2014. Retrieved 25 June 2014.
30. Elizabeth Miller Coyne (23 September 2016). "Huawei Exec: SDN's Become a 'Completely Meaningless Term'". Light Reading. Retrieved 25 September 2016.
31. "Software-Defined Networking (SDN) Definition". Opennetworking.org. Retrieved 26 October 2014.
32. "White Papers". Opennetworking.org. Retrieved 26 October 2014.
33. "SDN Architecture Overview" (PDF). Opennetworking.org. Retrieved 22

November 2014.

34. S.H. Yeganeh, Y. Ganjali, "Kandoo: A Framework for Efficient and Scalable Offloading of Control Applications," proceedings of HotSDN, Helsinki, Finland, 2012.
35. R. Ahmed, R. Boutaba, "Design considerations for managing wide area software defined networks," Communications Magazine, IEEE, vol. 52, no. 7, pp. 116–123, July 2014.
36. T. Koponen et al, "Onix: A Distributed Control Platform for Large scale Production Networks," proceedings USENIX, ser. OSDI'10, Vancouver, Canada, 2010.
37. D. Tuncer, M. Charalambides, S. Clayman, G. Pavlou, "Adaptive Resource Management and Control in Software Defined Networks," Network and Service Management, IEEE Transactions on, vol. 12, no. 1, pp. 18–33, March 2015.
38. B. Heller, R. Sherwood, and N. McKeown, "The Controller Placement Problem," proceedings of HotSDN'12, 2012.
39. Y.N. Hu, W.D. Wang, X.Y. Gong, X.R. Que, S.D. Cheng, "On the placement of controllers in software-defined networks," Journal of China Universities of Posts and Telecommunications, vol. 19, Supplement 2, no. 0, pp. 92 – 171, 2012.
40. F.J. Ros, P.M. Ruiz, "Five nines of southbound reliability in software defined networks," proceedings of HotSDN'14, 2014.
41. D. Tuncer, M. Charalambides, S. Clayman, G. Pavlou, "On the Placement of Management and Control Functionality in Software Defined Networks," proceedings of 2nd IEEE International Workshop on Management of SDN and NFV Systems (ManSDN/NFV), Barcelona, Spain, November 2015.
42. "OpenFlow: Proactive vs Reactive". NetworkStatic.net. Retrieved 2014-07-01.
43. "Reactive, Proactive, Predictive: SDN Models | F5 DevCentral". Devcentral.f5.com. Retrieved 2016-06-30.
44. Liyanage, Madhusanka (2015). Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture. UK: John Wiley. pp. 1–438. ISBN 978-1-118-90028-4.
45. Jose Costa-Requena, Jesús Llorente Santos, Vicent Ferrer Guasch, Kimmo Ahokas, Gopika Premsankar, Sakari Luukkainen, Ijaz Ahmed, Madhusanka Liyanage, Mika Ylianttila, Oscar López Pérez, Mikel Uriarte Itzazelaia, Edgardo Montes de Oca, SDN and NFV Integration in Generalized Mobile Network Architecture , in Proc. of European Conference on Networks and Communications (EUCNC), Paris, France. June 2015.
46. Madhusanka Liyanage, Mika Ylianttila, Andrei Gurtov, Securing the Control Channel of Software-Defined Mobile Networks , in Proc. of IEEE 15th International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), Sydney, Australia. June 2014.
47. Haranas, Mark (8 October 2016). "16 Hot Networking Products Putting The Sizzle In SD-WAN". CRN. Retrieved 1 November 2016.
48. "SD-WAN: What it is and why you'll use it one day". networkworld.com.

2016-02-10. Retrieved 2016-06-27.

49. Serries, William (12 September 2016). "SD-LAN et SD-WAN : Deux Approches Différentes pour le Software Defined Networking". ZDNet. Retrieved 1 November 2016.
50. Kerravala, Zeus (13 September 2016). "Aerohive Introduces the Software-defined LAN". Network World. Retrieved 1 November 2016.
51. Kreutz, Diego; Ramos, Fernando; Verissimo, Paulo (2013). "Towards secure and dependable software-defined networks". Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. pp. 50–60.
52. Scott-Hayward, Sandra; O'Callaghan, Gemma; Sezer, Sakir (2013). "SDN security: A survey". Future Networks and Services (SDN4FNS), 2013 IEEE SDN for. pp. 1–7.
53. Benton, Kevin; Camp, L Jean; Small, Chris (2013). "Openflow vulnerability assessment". Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. pp. 151–152.
54. Giotis, K; Argyropoulos, Christos; Androulidakis, Georgios; Kalogeras, Dimitrios; Maglaris, Vasilis (2014). "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments". Computer Networks. 62: 122–136.
55. Braga, Rodrigo; Mota, Edjard; Passito, Alexandre (2010). "Lightweight DDoS flooding attack detection using NOX/OpenFlow". Local Computer Networks (LCN), 2010 IEEE 35th Conference on. pp. 408–415.
56. Feamster, Nick (2010). "Outsourcing home network security". Proceedings of the 2010 ACM SIGCOMM workshop on Home networks. pp. 37–42.
57. Jin, Ruofan & Wang, Bing (2013). "Malware detection for mobile devices using software-defined networking". Research and Educational Experiment Workshop (GREE), 2013 Second GENI. 81-88.
58. Jafarian, Jafar Haadi; Al-Shaer, Ehab; Duan, Qi (2012). "Openflow random host mutation: transparent moving target defense using software defined networking". Proceedings of the first workshop on Hot topics in software defined networks. pp. 127–132.
59. Kampanakis, Panos; Perros, Harry; Beyene, Tsegereda. SDN-based solutions for Moving Target Defense network protection (PDF). Retrieved 23 July 2014.
60. Sherwood, Rob; Gibb, Glen; Yap, Kok-Kiong; Appenzeller, Guido; Casado, Martin; McKeown, Nick; Parulkar, Guru (2009). "Flowvisor: A network virtualization layer". OpenFlow Switch Consortium, Tech. Rep.
61. Al-Shaer, Ehab & Al-Haj, Saeed (2010). "FlowChecker: Configuration analysis and verification of federated OpenFlow infrastructures". Proceedings of the 3rd ACM workshop on Assurable and usable security configuration. pp. 37–44.
62. Canini, Marco; Venzano, Daniele; Peresini, Peter; Kostic, Dejan; Rexford, Jennifer; et al. (2012). A NICE Way to Test OpenFlow Applications. NSDI. pp. 127–140.

63. Bernardo and Chua (2015). Introduction and Analysis of SDN and NFV Security Architecture (SA-SECA). 29th IEEE AINA 2015. pp. 796–801.

CHAPTER 5

# Network Protocols

## Chapter Contents

- **List of Network Protocols**
- **Routing Protocol**
- **File Transfer Protocol**
- **Transmission Control Protocol**
- **Hypertext Transfer Protocol**
- **Network Time Protocol**

Robust transmission protocol is a protocol or system that has an ability to withstand changes in a procedure or recover from a range of exceptional inputs and situations in a given environment. The scenario here elaborates that a company called Microwave Infotech Ltd is setting up a LAN with a gateway to a WAN and the Internet, and are considering either SNA or TCP/IP as the network protocol thus having to justify why Microwave selected TCP/IP.

## LIST OF NETWORK PROTOCOLS

The following articles contain lists of network protocols in various formats.

- Protocol stack
- WIFI/WIMAX Protocols
- Bluetooth protocol
- Fibre Channel network protocols
- Internet Protocol Suite or TCP/IP model or TCP/IP stack
- OSI protocols family of information exchange standards developed jointly by the ISO and the ITU-T

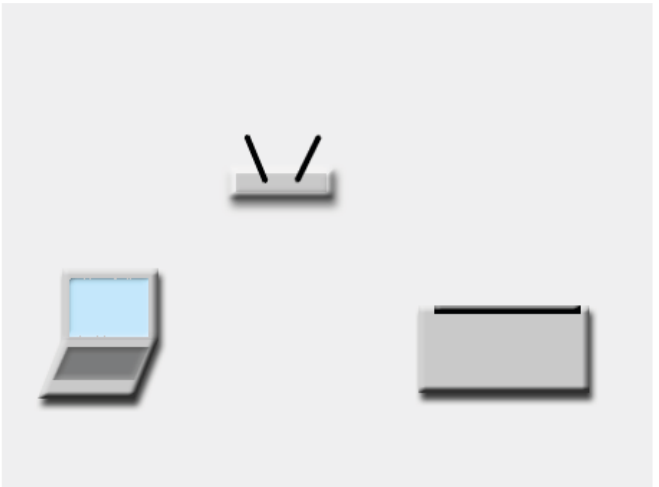
- Routing protocols
- List of IP protocol numbers, protocol numbers used in the Protocol field of the IPv4 header and the Next Header field of IPv6 header
- Yahoo! Messenger, underlying protocol used by the Yahoo messenger
- RTPS protocol, an interoperability protocol
- SSH Secure Shell
- SMB Server Message Block, one version of which was also known as CIFS (Common Internet File System)
- FTP File Transfer Protocol
- SMTP Simple Mail Transfer Protocol
- TCP Transmission Control Protocol
- Telnet Teletype Network
- HTTP Hyper Text Transfer Protocol
- HTTPs Secure Hyper Text Transfer Protocol
- POP Post Office Protocol
- HTCPCP Hyper Text Coffee Pot Control Protocol
- MTP Media Transfer Protocol
- SFTP Secure File Transfer Protocol
- SSL Secure Socket Layer
- TLS Transport Layer Security
- E6 Ethernet globalization protocols
- NTP Network time protocol
- PPP Point to Point Protocol
- NNTP Network News Transfer Protocol
- QOTD Quote Of The Day
- IMAP Internet Message Access Protocol
- Bitcoin Protocol Protocol for Bitcoin transactions and transfers on the web

## WI-FI

Wi-Fi or WiFi is a technology for wireless local area networking with devices based on the IEEE 802.11 standards. Wi-Fi is a trademark of the Wi-Fi Alliance, which restricts the use of the term Wi-Fi Certified to products that successfully complete interoperability certification testing.

Devices that can use Wi-Fi technology include personal computers, video-game consoles, smartphones, digital cameras, tablet computers, digital audio players and modern printers. Wi-Fi compatible devices can connect to the Internet via a WLAN network and a wireless access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a

single room with walls that block radio waves, or as large as many square kilometres achieved by using multiple overlapping access points.



Depiction of a device sending information wirelessly to another device, both connected to the local network, in order to print a document

Wi-Fi most commonly uses the 2.4 gigahertz (12 cm) UHF and 5 gigahertz (6 cm) SHF ISM radio bands. Having no physical connections, it is more vulnerable to attack than wired connections, such as Ethernet. Web pages that use Transport Layer Security (TLS) are secure, but unencrypted Internet access can easily be detected by intruders. For protection, Wi-Fi has adopted various encryption technologies. The early encryption Wired Equivalent Privacy (WEP) proved easy to break. Higher quality protocols, such as Wi-Fi Protected Access (WPA, WPA2) were added later. An optional feature added in 2007, called Wi-Fi Protected Setup (WPS), had a serious flaw that allowed an attacker to recover the router's password. The Wi-Fi Alliance has since updated its test plan and certification program to ensure all newly certified devices resist attacks.

## Etymology

The name Wi-Fi, commercially used at least as early as August 1999, was coined by the brand-consulting firm Interbrand. The Wi-Fi Alliance had hired Interbrand to create a name that was "a little catchier than 'IEEE 802.11b Direct Sequence.' " Phil Belanger, a founding member of the Wi-Fi Alliance who presided over the selection of the name "Wi-Fi," has stated that Interbrand invented Wi-Fi as a pun upon the word hi-fi

Interbrand also created the Wi-Fi logo. The yin-yang Wi-Fi logo indicates the certification of a product for interoperability.

The Wi-Fi Alliance used the nonsense advertising slogan "The Standard for Wireless Fidelity" for a short time after the brand name was created, leading to the misconception that Wi-Fi was an abbreviation of "Wireless Fidelity." The name was however never officially "Wireless Fidelity". Nevertheless, the Wi-Fi Alliance was also called the

"Wireless Fidelity Alliance Inc" in some publications and the IEEE's own website has stated "WiFi is a short name for Wireless Fidelity".

Non-Wi-Fi technologies intended for fixed points, such as Motorola Canopy, are usually described as fixed wireless. Alternative wireless technologies include mobile phone standards, such as 2G, 3G, 4G, and LTE.

The name is often written as **WiFi**, **Wifi**, or **wifi**, but these are not approved by the Wi-Fi Alliance.

### *Wi-Fi ad-Hoc Mode*

Wi-Fi nodes operating in ad-hoc mode refers to devices talking directly to each other without the need to first talk to an access point (also known as base station). Ad-hoc mode was first invented and realized by Chai K. Toh in his 1996 invention of Wi-Fi ad-hoc routing, implemented on Lucent WaveLAN 802.11a wireless on IBM ThinkPads over a size nodes scenario spanning a region of over a mile. The success was recorded in Mobile Computing magazine and later published formally in IEEE Transactions on Wireless Communications.

## Wi-Fi Certification

The IEEE does not test equipment for compliance with their standards. The non-profit Wi-Fi Alliance was formed in 1999 to fill this void — to establish and enforce standards for interoperability and backward compatibility, and to promote wireless local-area-network technology. As of 2010, the Wi-Fi Alliance consisted of more than 375 companies from around the world. The Wi-Fi Alliance enforces the use of the Wi-Fi brand to technologies based on the IEEE 802.11 standards from the IEEE. This includes wireless local area network (WLAN) connections, device to device connectivity (such as Wi-Fi Peer to Peer aka Wi-Fi Direct), Personal area network (PAN), local area network (LAN) and even some limited wide area network (WAN) connections. Manufacturers with membership in the Wi-Fi Alliance, whose products pass the certification process, gain the right to mark those products with the Wi-Fi logo.

Specifically, the certification process requires conformance to the IEEE 802.11 radio standards, the WPA and WPA2 security standards, and the EAP authentication standard. Certification may optionally include tests of IEEE 802.11 draft standards, interaction with cellular-phone technology in converged devices, and features relating to security set-up, multimedia, and power-saving.

Not every Wi-Fi device is submitted for certification. The lack of Wi-Fi certification does not necessarily imply that a device is incompatible with other Wi-Fi devices. The Wi-Fi Alliance may or may not sanction derivative terms, such as Super Wi-Fi, coined by the US Federal Communications Commission (FCC) to describe proposed networking in the UHF TV band in the US.

## IEEE 802.11 Standard




This Netgear Wi-Fi router contains dual bands for transmitting the 802.11 standard across the 2.4 and 5 GHz spectrums.

The IEEE 802.11 standard is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5, and 60 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand. While each amendment is officially revoked when it is incorporated in the latest version of the standard, the corporate world tends to market to the revisions because they concisely denote capabilities of their products. As a result, in the market place, each revision tends to become its own standard.

## Uses




A Japanese sticker indicating to the public that a location is within range of a Wi-Fi network. A dot with curved lines radiating from it is a common symbol for Wi-Fi, representing a point transmitting a signal.

To connect to a Wi-Fi LAN, a computer has to be equipped with a wireless network interface controller. The combination of computer and interface controller is called a station. For all stations that share a single radio frequency communication channel, transmissions on this channel are received by all stations within range. The transmission is not guaranteed to be delivered and is therefore a best-effort delivery mechanism. A carrier wave is used to transmit the data. The data is organised in packets on an Ethernet link, referred to as "Ethernet frames".

## Internet Access

Wi-Fi technology may be used to provide Internet access to devices that are within the range of a wireless network that is connected to the Internet. The coverage of one or more interconnected access points (hotspots) can extend from an area as small as a few rooms to as large as many square kilometres. Coverage in the larger area may require a group of access points with overlapping coverage. For example, public outdoor Wi-Fi technology has been used successfully in wireless mesh networks in London, UK. An international example is Fon.

Wi-Fi provides service in private homes, businesses, as well as in public spaces at Wi-Fi hotspots set up either free-of-charge or commercially, often using a captive portal webpage for access. Organizations and businesses, such as airports, hotels, and restaurants, often provide free-use hotspots to attract customers. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access.

Routers that incorporate a digital subscriber line modem or a cable modem and a Wi-Fi access point, often set up in homes and other buildings, provide Internet access and internetworking to all devices connected to them, wirelessly or via cable.

Similarly, battery-powered routers may include a cellular Internet radiomodem and Wi-Fi access point. When subscribed to a cellular data carrier, they allow nearby Wi-Fi stations to access the Internet over 2G, 3G, or 4G networks using the tethering technique. Many smartphones have a built-in capability of this sort, including those based on Android, BlackBerry, Bada, iOS (iPhone), Windows Phone and Symbian, though carriers often disable the feature, or charge a separate fee to enable it, especially for customers with unlimited data plans. "Internet packs" provide standalone facilities of this type as well, without use of a smartphone; examples include the MiFi- and WiBro-branded devices. Some laptops that have a cellular modem card can also act as mobile Internet Wi-Fi access points.

Wi-Fi also connects places that normally don't have network access, such as kitchens and garden sheds.

## City-wide Wi-Fi

In the early 2000s, many cities around the world announced plans to construct citywide Wi-Fi networks. There are many successful examples; in 2004, Mysore became India's first Wi-Fi-enabled city. A company called WiFiyNet has set up hotspots in Mysore, covering the complete city and a few nearby villages.

In 2005, St. Cloud, Florida and Sunnyvale, California, became the first cities in the United States to offer citywide free Wi-Fi (from MetroFi). Minneapolis has generated $1.2 million in profit annually for its provider.




An outdoor Wi-Fi access point

In May 2010, London, UK, Mayor Boris Johnson pledged to have London-wide Wi-Fi by 2012. Several boroughs including Westminster and Islington already had extensive outdoor Wi-Fi coverage at that point.

Officials in South Korea's capital are moving to provide free Internet access at more than 10,000 locations around the city, including outdoor public spaces, major streets and densely populated residential areas. Seoul will grant leases to KT, LG Telecom and SK Telecom. The companies will invest $44 million in the project, which was to be completed in 2015.

## Campus-Wide Wi-Fi

Many traditional university campuses in the developed world provide at least partial Wi-Fi coverage. Carnegie Mellon University built the first campus-wide wireless Internet network, called Wireless Andrew, at its Pittsburgh campus in 1993 before Wi-Fi branding originated. By February 1997 the CMU wifi zone was fully operational. Many universities collaborate in providing Wi-Fi access to students and staff through the eduroam international authentication infrastructure.

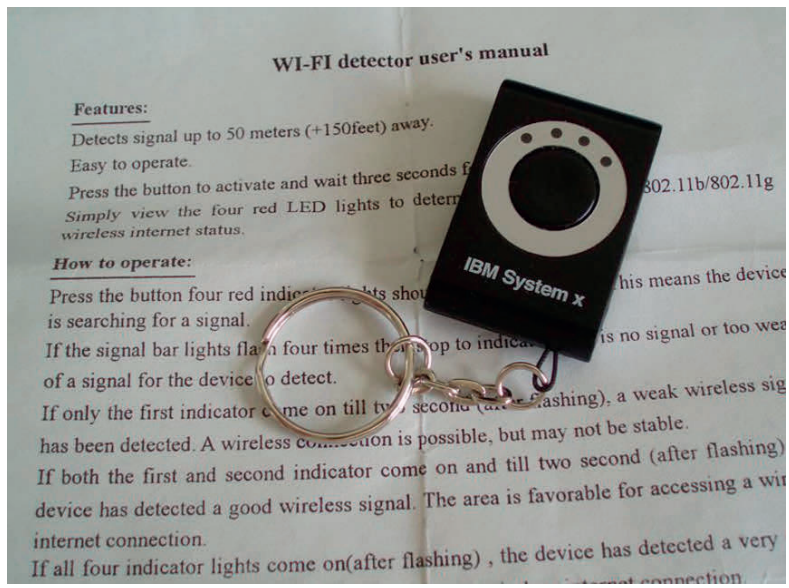
## Direct computer-to-Computer Communications

Wi-Fi also allows communications directly from one computer to another without an access point intermediary. This is called ad hoc Wi-Fi transmission. This wireless

ad hoc network mode has proven popular with multiplayer handheld game consoles, such as the Nintendo DS, PlayStation Portable, digital cameras, and other consumer electronics devices. Some devices can also share their Internet connection using ad hoc, becoming hotspots or "virtual routers".

Similarly, the Wi-Fi Alliance promotes the specification Wi-Fi Direct for file transfers and media sharing through a new discovery- and security-methodology. Wi-Fi Direct launched in October 2010.

Another mode of direct communication over Wi-Fi is Tunneled Direct Link Setup (TDLS), which enables two devices on the same Wi-Fi network to communicate directly, instead of via the access point.




A keychain-size Wi-Fi detector

## Wi-Fi radio Spectrum

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones, and Bluetooth devices.

Spectrum assignments and operational limitations are not consistent worldwide: Australia and Europe allow for an additional two channels (12, 13) beyond the 11 permitted in the United States for the 2.4 GHz band, while Japan has three more (12–14). In the US and other countries, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations.

A Wi-Fi signal occupies five channels in the 2.4 GHz band. Any two channel numbers that differ by five or more, such as 2 and 7, do not overlap. The oft-repeated adage that

channels 1, 6, and 11 are the only non-overlapping channels is, therefore, not accurate. Channels 1, 6, and 11 are the only group of three non-overlapping channels in North America and the United Kingdom. In Europe and Japan using Channels 1, 5, 9, and 13 for 802.11g and 802.11n is recommended.

802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap.

### *Interference*

Wi-Fi connections can be disrupted or the Internet speed lowered by having other devices in the same area. Many 2.4 GHz 802.11b and 802.11g access-points default to the same channel on initial startup, contributing to congestion on certain channels. Wi-Fi pollution, or an excessive number of access points in the area, especially on the neighboring channel, can prevent access and interfere with other devices' use of other access points, caused by overlapping channels in the 802.11g/b spectrum, as well as with decreased signal-to-noise ratio (SNR) between access points. This can become a problem in high-density areas, such as large apartment complexes or office buildings with many Wi-Fi access points. It is advised to only use channel 1-6-11.

Additionally, other devices use the 2.4 GHz band: microwave ovens, ISM band devices, security cameras, ZigBee devices, Bluetooth devices, video senders, cordless phones, baby monitors, and, in some countries, amateur radio, all of which can cause significant additional interference. It is also an issue when municipalities or other large entities (such as universities) seek to provide large area coverage.

## Service Set Identifier (SSID)

In addition to running on different channels, multiple Wi-Fi networks can share channels.

A service set is the set of all the devices associated with a particular Wi-Fi network. The service set can be local, independent, extended or mesh.

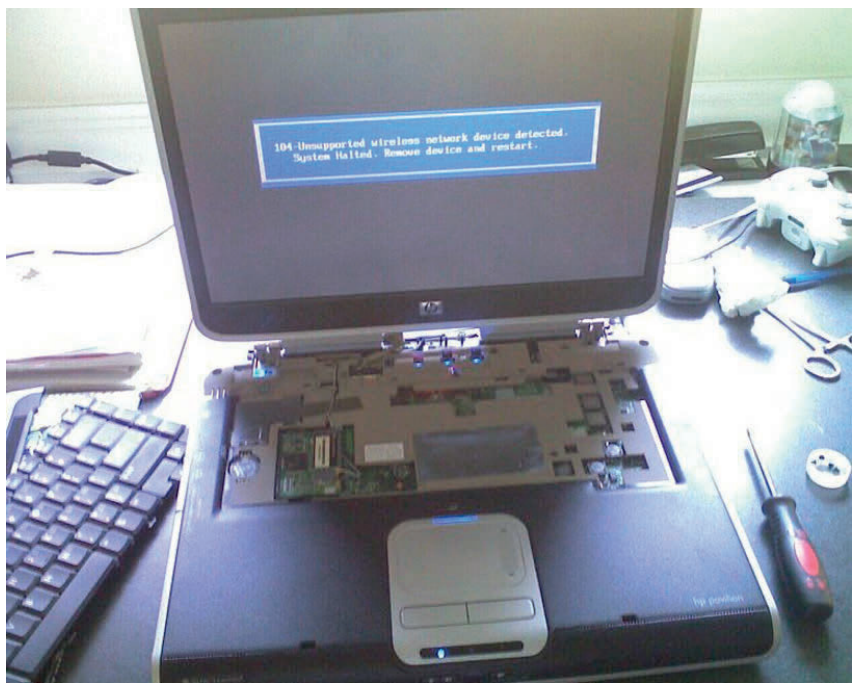
Each service set has an associated identifier, the 32-byte Service Set Identifier (SSID), which identifies the particular network. The SSID is configured within the devices that are considered part of the network, and it is transmitted in the packets. Receivers ignore wireless packets from networks with a different SSID.

## Throughput

As the 802.11 specifications evolved to support higher throughput, the bandwidth requirements also increased to support them. 802.11n uses double the radio spectrum/bandwidth (40 MHz) compared to 802.11a or 802.11g (20 MHz).76 This means there can be only one 802.11n network on the 2.4 GHz band at a given location, without interference to/from other WLAN traffic. 802.11n can also be set to limit itself to 20 MHz bandwidth to prevent interference in dense community.

Many newer consumer devices support the latest 802.11ac standard, which uses the 5 GHz band exclusively and is capable of multi-station WLAN throughput of at least 1 gigabit per second. According to a study, devices with the 802.11ac specification were expected to be common by 2015 with an estimated one billion spread around the world.

## Hardware



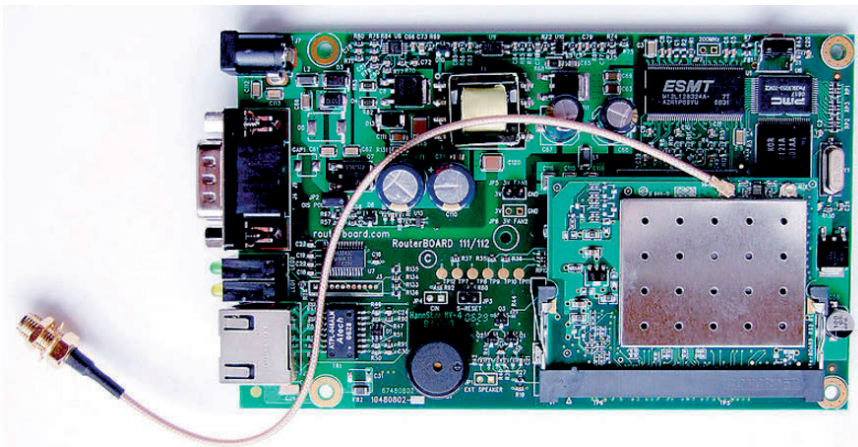

Wi-Fi whitelist triggered on an HP laptop

Wi-Fi allows cheaper deployment of local area networks (LANs). Also, spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs. However, building walls of certain materials, such as stone with high metal content, can block Wi-Fi signals.

Manufacturers are building wireless network adapters into most laptops. The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in even more devices.

Different competitive brands of access points and client network-interfaces can inter-operate at a basic level of service. Products designated as "Wi-Fi Certified" by the Wi-Fi Alliance are backward compatible. Unlike mobile phones, any standard Wi-Fi device will work anywhere in the world.

## *Standard Devices*




An embedded RouterBoard 112 with U.FL-RSMA pigtail and R52 mini PCI Wi-Fi card widely used by wireless Internet service providers (WISPs) in the Czech Republic




OSBRiDGE 3GN – 802.11n Access Point and UMTS/GSM Gateway in one device




An Atheros draft-N Wi-Fi adapter with built in Bluetooth on a Sony Vaio E series laptop




USB wireless adapter

A wireless access point (WAP) connects a group of wireless devices to an adjacent wired LAN. An access point resembles a network hub, relaying data between connected wireless devices in addition to a (usually) single connected wired device, most often an Ethernet hub or switch, allowing wireless devices to communicate with other wired devices.

Wireless adapters allow devices to connect to a wireless network. These adapters connect to devices using various external or internal interconnects such as PCI, miniPCI, USB, ExpressCard, Cardbus and PC Card. As of 2010, most newer laptop computers come equipped with built in internal adapters.

Wireless routers integrate a Wireless Access Point, Ethernet switch, and internal router firmware application that provides IP routing, NAT, and DNS forwarding through an integrated WAN-interface. A wireless router allows wired and wireless Ethernet LAN devices to connect to a (usually) single WAN device such as a cable modem or a DSL modem. A wireless router allows all three devices, mainly the access point and router, to be configured through one central utility. This utility is usually an integrated web

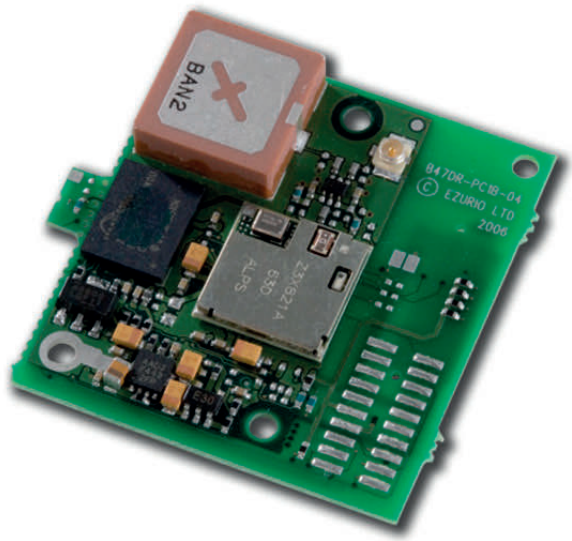
server that is accessible to wired and wireless LAN clients and often optionally to WAN clients. This utility may also be an application that is run on a computer, as is the case with as Apple's AirPort, which is managed with the AirPort Utility on Mac OS X and iOS.

Wireless network bridges connect a wired network to a wireless network. A bridge differs from an access point: an access point connects wireless devices to a wired network at the data-link layer. Two wireless bridges may be used to connect two wired networks over a wireless link, useful in situations where a wired connection may be unavailable, such as between two separate homes or for devices which do not have wireless networking capability (but have wired networking capability), such as consumer entertainment devices; alternatively, a wireless bridge can be used to enable a device which supports a wired connection to operate at a wireless networking standard which is faster than supported by the wireless network connectivity feature (external dongle or inbuilt) supported by the device (e.g. enabling Wireless-N speeds (up to the maximum supported speed on the wired Ethernet port on both the bridge and connected devices including the wireless access point) for a device which only supports Wireless-G). A dual-band wireless bridge can also be used to enable 5 GHz wireless network operation on a device which only supports 2.4 GHz wireless networking functionality and has a wired Ethernet port.

Wireless range-extenders or wireless repeaters can extend the range of an existing wireless network. Strategically placed range-extenders can elongate a signal area or allow for the signal area to reach around barriers such as those pertaining in L-shaped corridors. Wireless devices connected through repeaters will suffer from an increased latency for each hop, as well as from a reduction in the maximum data throughput that is available. In addition, the effect of additional users using a network employing wireless range-extenders is to consume the available bandwidth faster than would be the case where but a single user migrates around a network employing extenders. For this reason, wireless range-extenders work best in networks supporting very low traffic throughput requirements, such as for cases where but a single user with a Wi-Fi equipped tablet migrates around the combined extended and non-extended portions of the total connected network. Additionally, a wireless device connected to any of the repeaters in the chain will have a data throughput that is also limited by the "weakest link" existing in the chain between where the connection originates and where the connection ends. Networks employing wireless extenders are also more prone to degradation from interference from neighboring access points that border portions of the extended network and that happen to occupy the same channel as the extended network.

The security standard, Wi-Fi Protected Setup, allows embedded devices with limited graphical user interface to connect to the Internet with ease. Wi-Fi Protected Setup has 2 configurations: The Push Button configuration and the PIN configuration. These embedded devices are also called The Internet of Things and are low-power, battery-operated embedded systems. A number of Wi-Fi manufacturers design chips and modules for embedded Wi-Fi, such as GainSpan.

### *Embedded Systems*




Embedded serial-to-Wi-Fi module

Increasingly in the last few years (particularly as of 2007), embedded Wi-Fi modules have become available that incorporate a real-time operating system and provide a simple means of wirelessly enabling any device which has and communicates via a serial port. This allows the design of simple monitoring devices. An example is a portable ECG device monitoring a patient at home. This Wi-Fi-enabled device can communicate via the Internet.

These Wi-Fi modules are designed by OEMs so that implementers need only minimal Wi-Fi knowledge to provide Wi-Fi connectivity for their products.

In June 2014 Texas Instruments introduced the first ARM Cortex-M4 microcontroller with an onboard dedicated Wi-Fi MCU, the SimpleLink CC3200. It makes embedded systems with Wi-Fi connectivity possible to build as single-chip devices, which reduces their cost and minimum size, making it more practical to build wireless-networked controllers into inexpensive ordinary objects.

## Range

The Wi-Fi signal range depends on the frequency band, radio power output, antenna gain and antenna type as well as the modulation technique. Line-of-sight is the thumbnail guide but reflection and refraction can have a significant impact.

An access point compliant with either 802.11b or 802.11g, using the stock antenna might have a range of 100 m (330 ft). The same radio with an external semi parabolic antenna (15 dB gain) might have a range over 20 miles.

Higher gain rating (dBi) indicates further deviation (generally toward the horizontal) from a theoretical, perfect isotropic radiator, and therefore the further the antenna can project a usable signal, as compared to a similar output power on a more isotropic

antenna. For example, an 8 dBi antenna used with a 100 mW driver will have a similar horizontal range to a 6 dBi antenna being driven at 500 mW. Note that this assumes that radiation in the vertical is lost; this may not be the case in some situations, especially in large buildings or within a waveguide. In the above example, a directional waveguide could cause the low power 6 dBi antenna to project much further in a single direction than the 8 dBi antenna which is not in a waveguide, even if they are both being driven at 100 mW.

IEEE 802.11n, however, can more than double the range. Range also varies with frequency band. Wi-Fi in the 2.4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block used by 802.11a (and optionally by 802.11n). On wireless routers with detachable antennas, it is possible to improve range by fitting upgraded antennas which have higher gain in particular directions. Outdoor ranges can be improved to many kilometers through the use of high gain directional antennas at the router and remote device(s). In general, the maximum amount of power that a Wi-Fi device can transmit is limited by local regulations, such as FCC Part 15 in the US. Equivalent isotropically radiated power (EIRP) in the European Union is limited to 20 dBm (100 mW).

To reach requirements for wireless LAN applications, Wi-Fi has fairly high power consumption compared to some other standards. Technologies such as Bluetooth (designed to support wireless personal area network (PAN) applications) provide a much shorter propagation range between 1 and 100 m and so in general have a lower power consumption. Other low-power technologies such as ZigBee have fairly long range, but much lower data rate. The high power consumption of Wi-Fi makes battery life in mobile devices a concern.

Researchers have developed a number of “no new wires” technologies to provide alternatives to Wi-Fi for applications in which Wi-Fi’s indoor range is not adequate and where installing new wires (such as CAT-6) is not possible or cost-effective. For example, the ITU-T G.hn standard for high speed local area networks uses existing home wiring (coaxial cables, phone lines and power lines). Although G.hn does not provide some of the advantages of Wi-Fi (such as mobility or outdoor use), it is designed for applications (such as IPTV distribution) where indoor range is more important than mobility.

For the best performance, a number of people only recommend using wireless networking as a supplement to wired networking.

Due to the complex nature of radio propagation at typical Wi-Fi frequencies, particularly the effects of signal reflection off trees and buildings, algorithms can only approximately predict Wi-Fi signal strength for any given area in relation to a transmitter. This effect does not apply equally to long-range Wi-Fi, since longer links typically operate from towers that transmit above the surrounding foliage.

The practical range of Wi-Fi essentially confines mobile use to such applications as inventory-taking machines in warehouses or in retail spaces, barcode-reading devices at check-out stands, or receiving/shipping stations. Mobile use of Wi-Fi over wider ranges is limited, for instance, to uses such as in an automobile moving from one hotspot to another. Other wireless technologies are more suitable for communicating with moving vehicles.

### *Distance Records*

Distance records (using non-standard devices) include 382 km (237 mi) in June 2007, held by Ermanno Pietrosemoli and EsLaRed of Venezuela, transferring about 3 MB of data between the mountain-tops of El Águila and Platillon. The Swedish Space Agency transferred data 420 km (260 mi), using 6 watt amplifiers to reach an overhead stratospheric balloon.

## Multiple Access Points

Increasing the number of Wi-Fi access points provides network redundancy, better range, support for fast roaming and increased overall network-capacity by using more channels or by defining smaller cells. Except for the smallest implementations (such as home or small office networks), Wi-Fi implementations have moved toward "thin" access points, with more of the network intelligence housed in a centralized network appliance, relegating individual access points to the role of "dumb" transceivers. Outdoor applications may use mesh topologies.

When multiple access points are deployed they are often configured with the same SSID and security settings to form an "extended service set". Wi-Fi client devices will typically connect to the access point that can provide the strongest signal within that service set.

## Network Security

The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as Ethernet. With wired networking, one must either gain access to a building (physically connecting into the internal network), or break through an external firewall. To enable Wi-Fi, one merely needs to be within the range of the Wi-Fi network. Most business networks protect sensitive data and systems by attempting to disallow external access. Enabling wireless connectivity reduces security if the network uses inadequate or no encryption.

An attacker who has gained access to a Wi-Fi network router can initiate a DNS spoofing attack against any other user of the network by forging a response before the queried DNS server has a chance to reply.

## List of Bluetooth Protocols

The wireless data exchange standard Bluetooth uses a variety of protocols. Core protocols are defined by the trade organization Bluetooth SIG. Add protocols have been adopted from other standards bodies. This article gives an overview of the core protocols and those adopted protocols that are widely used.

The Bluetooth protocol stack is split in two parts: a "controller stack" containing the timing critical radio interface, and a "host stack" dealing with high level data. The controller stack is generally implemented in a low cost silicon device containing the Bluetooth radio and a microprocessor. The host stack is generally implemented as part

of an operating system, or as an installable package on top of an operating system. For integrated devices such as Bluetooth headsets, the host stack and controller stack can be run on the same microprocessor to reduce mass production costs; this is known as a hostless system.

## Controller Stack

### *Link layer*

The lowest layer of the Bluetooth protocol stack has no name (unlike Ethernet), but is responsible for transporting Bluetooth packets between devices on the piconet. Four "physical channels" are defined for each piconet: the basic piconet channel, which transports normal communication between devices; the adapted piconet channel, similar to the basic; the inquiry scan channel, for discovering Bluetooth devices; and the page scan channel, for connecting new devices. Each channel hops through the RF channels in a predetermined manner.

All packets have a "channel access code" header field which distinguishes the piconet from other piconets using the same RF channel. Additionally, packets in the basic and adapted piconet channels have the LT_ADDR header field, which specifies the packet's "logical transport." Logical transports only exist between the master and slave devices, never between slaves. Additionally, some logical transports can carry multiple logical links.

There are five types of logical transport:

### *Asynchronous Connection-Less (ACL)*

The normal type of radio link used for general data packets using a polling TDMA scheme to arbitrate access. ACL can carry packets of several types, which are distinguished by:

- Length (1, 3, or 5 time slots depending on required payload size)
- Forward error correction (optionally reducing the data rate in favour of reliability)
- Modulation (Enhanced Data Rate packets allow up to triple data rate by using a different RF modulation for the payload)

Each device receives a default ACL logical transport when it joins the piconet. The connection must be explicitly set up and accepted between two devices before packets can be transferred. Each ACL "logical transport" carries one or more ACL "logical links", which are distinguished by the Logical Link ID (LLID) field of the ACL header. The default ACL has two default logical links: ACL-C for LMP control signaling, and the default ACL-U for L2CAP.

ACL packets are retransmitted automatically if unacknowledged, allowing for correction of a radio link that is subject to interference. For isochronous data, the number of retransmissions can be limited by a flush timeout; but without using L2PLAY retransmission and flow control mode or EL2CAP, a higher layer must handle the packet loss.

ACL logical transports are disconnected if there is nothing received for the supervision timeout period; the default timeout is 20 seconds, but this may be modified by the master.

For legacy reasons, ACL and SCO logical transports share LT_ADDR's. Their packets are differentiated by timing.

### Synchronous Connection-Oriented (SCO)

The type of radio link used for voice data. A SCO link is a set of reserved timeslots on an existing ACL transport. Each device transmits encoded voice data in the reserved timeslot. There are no retransmissions, but forward error correction can be optionally applied. SCO packets may be sent every 1, 2 or 3 timeslots.

Unlike ACL, SCO data is streamed instead of framed, so no distinction exists between SCO logical transports and logical links.

### Active Slave Broadcast (ASB)

An implicit logical transport that carries broadcast L2CAP user data (but not L2CAP control commands). It uses the reserved LT_ADDR of 0, which it shares with Parked Slave Broadcast; their packets are differentiated by timing instead.

### Parked Slave Broadcast (PSB)

An implicit logical transport that can carry a subset of LMP and broadcast L2CAP data. It uses the LT_ADDR 0, so its packets are superficially indistinguishable from ASB packets. However, only clients that have been "parked" with LMP (involving closing all their logical transports) listen for PSB packets.

### Link Control Protocol (LC)

Used to communicate flow control, acknowledgement, and retransmission requests. It is embedded in the headers of logical transport protocols, except that ACL and SCO share an LC connection which can be carried in either's header.

### Link Manager Protocol (LMP)

Used to control the connections between two devices, including creating, modifying, and releasing logical transports and logical links, querying device abilities, "parking" devices, and power control. LMP is carried over the ACL-C logical link of the default ACL logical transport, or over PSB. Implemented in the controller.

### Low-Energy Link Layer (LELL)

This is the LMP equivalent for Bluetooth Low Energy (LE), but is simpler. It is implemented on the controller and manages advertisement, scanning, connection and security from a low-level, close to the hardware point of view from Bluetooth perspective.

### *Host Controller Interface (HCI)*

The pseudo-protocol referring to any standardized communication between the host stack (e.g., a PC or mobile phone OS) and the controller (the Bluetooth IC). An HCI decouples the host from the controller, allowing either to be swapped without affecting the other. Bluetooth defines several HCI standards, each for a different hardware interface to transfer the same commands, events, and data packets. The most commonly used are USB (in PCs) and UART (in mobile phones and PDAs).

It must expose enough functionality to allow the host: to discover, add, and manage devices on the piconet; to configure controller properties; to set up, manage, and release logical transports and links; and to write directly to the baseband's buffer for SCO and eSCO streaming.

In simple Bluetooth devices (e.g., headsets), the host stack and controller can be implemented on the same microprocessor. In this case an HCI serves no purpose, and often implemented only as an internal software interface.

## Host Stack

### *Logical Link Control and Adaptation Protocol (L2cap)*

**L2CAP** is used within the Bluetooth protocol stack. It passes packets to either the Host Controller Interface (HCI) or on a hostless system, directly to the ACL/ASB/PSB link.

L2CAP's functions include:

- Transporting data for higher layer protocols, including multiplexing multiple applications over a single link.
- Segmentation and reassembly of packets.
- Providing one-way transmission management of multicast data to a group of other Bluetooth devices.
- Quality of service (QoS) management for higher layer protocols.

It is channel-based, and control commands are sent on channel 0x0001. This signaling channel is available as soon as the default ACL-U logical link has been set up, and is used to set up additional channels. L2CAP channels can be connection-oriented or group-oriented, and are transported by ACL in the former case, or by ASB or PSB in the latter.

In basic mode, L2CAP provides packets with a payload configurable up to 64 kB, with 672 bytes as the default maximum transmission unit (MTU), and 48 bytes as the minimum mandatory supported MTU. In retransmission and flow control modes, L2CAP can be configured for reliable or asynchronous data per channel by performing retransmissions and CRC checks. Reliability in either of these modes is optionally and/or additionally guaranteed by the lower layer Bluetooth BDR/EDR air interface by configuring the number of retransmissions and flush timeout (time after which the radio will flush packets). In-order sequencing is guaranteed by the lower layer.

The EL2CAP specification adds an additional enhanced retransmission mode (ERTM) to the core specification, which is an improved version of retransmission and flow control modes. ERTM is required when using an AMP (Alternate MAC/PHY), such as 802.11abgn.

## Bluetooth Network Encapsulation Protocol (BNEP)

**BNEP** is used for delivering network packets on top of L2CAP. This protocol is used by the personal area networking (PAN) profile. BNEP performs a similar function to Subnetwork Access Protocol (SNAP) in Wireless LAN.

In the protocol stack, BNEP is bound to L2CAP

## Radio Frequency Communication (Rfcomm)

The Bluetooth protocol RFCOMM is a simple set of transport protocols, made on top of the L2CAP protocol, providing emulated RS-232 serial ports (up to sixty simultaneous connections to a Bluetooth device at a time). The protocol is based on the ETSI standard TS 07.10.

RFCOMM is sometimes called serial port emulation. The Bluetooth serial port profile is based on this protocol.

RFCOMM provides a simple reliable data stream to the user, similar to TCP. It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth.

Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM

In the protocol stack, RFCOMM is bound to L2CAP.

## Service Discovery Protocol (SDP)

Used to allow devices to discover what services are supported by each other, and what parameters to use to connect to them. For example, when connecting a mobile phone to a Bluetooth headset, SDP will be used to determine which Bluetooth profiles are supported by the headset (headset profile, hands free profile, advanced audio distribution profile, etc.) and the protocol multiplexer settings needed to connect to each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128).

In the protocol stack, SDP is bound to L2CAP.

## Telephony Control Protocol Specification (TCS)

Also referred to as telephony control protocol specification binary (TCS binary)

Used to set up and control speech and data calls between Bluetooth devices. The protocol is based on the ITU-T standard Q.931, with the provisions of Annex D applied, making only the minimum changes necessary for Bluetooth.

TCP is used by the intercom (ICP) and cordless telephony (CTP) profiles.

### *Audio/Video Control Transport Protocol (AVCTP)*

Used by the remote control profile to transfer AV/C commands over an L2CAP channel. The music control buttons on a stereo headset use this protocol to control the music player

In the protocol stack, AVCTP is bound to L2CAP.

### *Audio/Video Distribution Transport Protocol (AVDTP)*

Used by the advanced audio distribution profile to stream music to stereo headsets over an L2CAP channel. Intended to be used by video distribution profile.

In the protocol stack, AVDTP is bound to L2CAP.

### *Object Exchange (OBEX)*

Object exchange (OBEX; also termed IrOBEX) is a communications protocol that facilitates the exchange of binary objects between devices. It is maintained by the Infrared Data Association but has also been adopted by the Bluetooth Special Interest Group and the SyncML wing of the Open Mobile Alliance (OMA).

In Bluetooth, OBEX is used for many profiles that require simple data exchange (e.g., object push, file transfer, basic imaging, basic printing, phonebook access, etc.). In the protocol stack, OBEX is bound to RFCOMM.

### *Low Energy Attribute Protocol (ATT)*

Similar in scope to SDP but specially adapted and simplified for Low Energy Bluetooth. It allows a client to read and/or write certain attributes exposed by the server in a non-complex, low-power friendly manner.

In the protocol stack, ATT is bound to L2CAP.

## ROUTING PROTOCOL

A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.

Although there are many types of routing protocols, three major classes are in widespread use on IP networks:

Interior gateway protocols type 1, link-state routing protocols, such as OSPF and IS-IS

Interior gateway protocols type 2, distance-vector routing protocols, such as Routing Information Protocol, RIPv2, IGRP.

Exterior gateway protocols are routing protocols used on the Internet for exchanging routing information between Autonomous Systems, such as Border Gateway Protocol (BGP), Path Vector Routing Protocol.

Exterior gateway protocols should not be confused with Exterior Gateway Protocol (EGP), an obsolete routing protocol.

Many routing protocols are defined in documents called RFCs.

Some versions of the Open System Interconnection (OSI) networking model distinguish routing protocols in a special sublayer of the Network Layer (Layer 3).

The specific characteristics of routing protocols include the manner in which they avoid routing loops, the manner in which they select preferred routes, using information about hop costs, the time they require to reach routing convergence, their scalability, and other factors.

## OSI Layer Designation

Routing protocols, according to the OSI routing framework, are layer management protocols for the network layer, regardless of their transport mechanism:

- IS-IS runs on the data link layer (Layer 2)
- Open Shortest Path First (OSPF) is encapsulated in IP, but runs only on the IPv4 subnet, while the IPv6 version runs on the link using only link-local addressing.
- IGRP, and EIGRP are directly encapsulated in IP. EIGRP uses its own reliable transmission mechanism, while IGRP assumed an unreliable transport.
- RIP runs over UDP
- BGP runs over TCP

## Interior Gateway Protocols

Interior gateway protocols (IGPs) exchange routing information within a single routing domain. Examples of IGPs include:

- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP)
- Intermediate System to Intermediate System (IS-IS)
- Enhanced Interior Gateway Routing Protocol (EIGRP)[a]

# FILE TRANSFER PROTOCOL

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network.

FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves

with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead, but is technologically different.

The first FTP client applications were command-line programs developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems. Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as web page editors.

## Protocol Overview

## Communication and Data Transfer

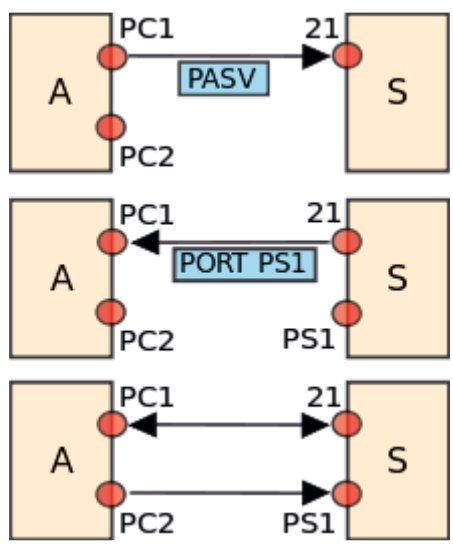



Illustration of starting a passive connection using port 21

FTP may run in active or passive mode, which determines how the data connection is established. In both cases, the client creates a TCP control connection from a random, usually an unprivileged, port N to the FTP server command port 21.

- In active mode, the client starts listening for incoming data connections from the server on port M. It sends the FTP command PORT M to inform the server on which port it is listening. The server then initiates a data channel to the client from its port 20, the FTP server data port.
- In situations where the client is behind a firewall and unable to accept incoming TCP connections, passive mode may be used. In this mode, the client uses the control connection to send a PASV command to the server and then receives

a server IP address and server port number from the server, which the client then uses to open a data connection from an arbitrary client port to the server IP address and server port number received.

Both modes were updated in September 1998 to support IPv6. Further changes were introduced to the passive mode at that time, updating it to extended passive mode.

The server responds over the control connection with three-digit status codes in ASCII with an optional text message. For example, "200" (or "200 OK") means that the last command was successful. The numbers represent the code for the response and the optional text represents a human-readable explanation or request (e.g. <Need account for storing file>). An ongoing transfer of file data over the data connection can be aborted using an interrupt message sent over the control connection.

While transferring data over the network, four data representations can be used:

- ASCII mode: Used for text. Data is converted, if needed, from the sending host's character representation to "8-bit ASCII" before transmission, and (again, if necessary) to the receiving host's character representation. As a consequence, this mode is inappropriate for files that contain data other than plain text.
- Image mode (commonly called Binary mode): The sending machine sends each file byte for byte, and the recipient stores the bytestream as it receives it. (Image mode support has been recommended for all implementations of FTP).
- EBCDIC mode: Used for plain text between hosts using the EBCDIC character set.
- Local mode: Allows two computers with identical setups to send data in a proprietary format without the need to convert it to ASCII.

For text files, different format control and record structure options are provided. These features were designed to facilitate files containing Telnet or ASA.

Data transfer can be done in any of three modes:

- Stream mode: Data is sent as a continuous stream, relieving FTP from doing any processing. Rather, all processing is left up to TCP. No End-of-file indicator is needed, unless the data is divided into records.
- Block mode: FTP breaks the data into several blocks (block header, byte count, and data field) and then passes it on to TCP.
- Compressed mode: Data is compressed using a simple algorithm (usually run-length encoding).

Some FTP software also implements a DEFLATE-based compressed mode, sometimes called "Mode Z" after the command that enables it. This mode was described in an Internet Draft, but not standardized.

## Login

FTP login utilizes a normal username and password scheme for granting access. The username is sent to the server using the USER command, and the password is sent using

the PASS command. If the information provided by the client is accepted by the server, the server will send a greeting to the client and the session will commence. If the server supports it, users may log in without providing login credentials, but the same server may authorize only limited access for such sessions.

## Anonymous FTP

A host that provides an FTP service may provide anonymous FTP access. Users typically log into the service with an 'anonymous' (lower-case and case-sensitive in some FTP servers) account when prompted for user name. Although users are commonly asked to send their email address instead of a password, no verification is actually performed on the supplied data. Many FTP hosts whose purpose is to provide software updates will allow anonymous logins.

## NAT and Firewall Traversal

FTP normally transfers data by having the server connect back to the client, after the PORT command is sent by the client. This is problematic for both NATs and firewalls, which do not allow connections from the Internet towards internal hosts. For NATs, an additional complication is that the representation of the IP addresses and port number in the PORT command refer to the internal host's IP address and port, rather than the public IP address and port of the NAT.

There are two approaches to this problem. One is that the FTP client and FTP server use the PASV command, which causes the data connection to be established from the FTP client to the server. This is widely used by modern FTP clients. Another approach is for the NAT to alter the values of the PORT command, using an application-level gateway for this purpose.

## Differences from HTTP

HTTP essentially fixes the bugs in FTP that made it inconvenient to use for many small ephemeral transfers as are typical in web pages.

FTP has a stateful control connection which maintains a current working directory and other flags, and each transfer requires a secondary connection through which the data are transferred. In "passive" mode this secondary connection is from client to server, whereas in the default "active" mode this connection is from server to client. This apparent role reversal when in active mode, and random port numbers for all transfers, is why firewalls and NAT gateways have such a hard time with FTP. HTTP is stateless and multiplexes control and data over a single connection from client to server on well-known port numbers, which trivially passes through NAT gateways and is simple for firewalls to manage.

Setting up an FTP control connection is quite slow due to the round-trip delays of sending all of the required commands and awaiting responses, so it is customary to bring up a control connection and hold it open for multiple file transfers rather than

drop and re-establish the session afresh each time. In contrast, HTTP originally dropped the connection after each transfer because doing so was so cheap. While HTTP has subsequently gained the ability to reuse the TCP connection for multiple transfers, the conceptual model is still of independent requests rather than a session.

When FTP is transferring over the data connection, the control connection is idle. If the transfer takes long enough, the firewall or NAT may decide that the control connection is dead and stop tracking it, effectively breaking the connection and confusing the download. The single HTTP connection is only idle between requests and it is normal and expected for such connections to be dropped after a time-out.

### Web Browser Support

Most common web browsers can retrieve files hosted on FTP servers, although they may not support protocol extensions such as FTPS.When an FTP—rather than an HTTP—URL is supplied, the accessible contents on the remote server are presented in a manner that is similar to that used for other web content. A full-featured FTP client can be run within Firefox in the form of an extension called FireFTP.

## TRANSMISSION CONTROL PROTOCOL

The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating by an IP network. Major Internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP. Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that emphasizes reduced latency over reliability.

### Network Function

The Transmission Control Protocol provides a communication service at an intermediate level between an application program and the Internet Protocol. It provides host-to-host connectivity at the Transport Layer of the Internet model. An application does not need to know the particular mechanisms for sending data via a link to another host, such as the required packet fragmentation on the transmission medium. At the transport layer, the protocol handles all handshaking and transmission details and just presents an abstraction of the network connection to the application.

At the lower levels of the protocol stack, due to network congestion, traffic load balancing, or other unpredictable network behaviour, IP packets may be lost, duplicated, or delivered out of order. TCP detects these problems, requests re-transmission of lost data, rearranges out-of-order data and even helps minimise network congestion to reduce the occurrence of the other problems. If the data still remains undelivered, its source is notified of this failure. Once the TCP receiver has reassembled the sequence of octets

originally transmitted, it passes them to the receiving application. Thus, TCP abstracts the application's communication from the underlying networking details.

TCP is used extensively by many applications available by internet, including the World Wide Web (WWW), E-mail, File Transfer Protocol, Secure Shell, peer-to-peer file sharing, and streaming media applications.

TCP is optimised for accurate delivery rather than timely delivery. Therefore, TCP sometimes incurs relatively long delays (on the order of seconds) while waiting for out-of-order messages or re-transmissions of lost messages. It is not particularly suitable for real-time applications such as Voice over IP. For such applications, protocols like the Real-time Transport Protocol (RTP) operating over the User Datagram Protocol (UDP) are usually recommended instead.

TCP is a reliable stream delivery service which guarantees that all bytes received will be identical with bytes sent and in the correct order. Since packet transfer by many networks is not reliable, a technique known as 'positive acknowledgement with re-transmission' is used to guarantee reliability of packet transfers. This fundamental technique requires the receiver to respond with an acknowledgement message as it receives the data. The sender keeps a record of each packet it sends and maintains a timer from when the packet was sent. The sender re-transmits a packet if the timer expires before the message has been acknowledged. The timer is needed in case a packet gets lost or corrupted.

While IP handles actual delivery of the data, TCP keeps track of 'segments' - the individual units of data transmission that a message is divided into for efficient routing through the network. For example, when an HTML file is sent from a web server, the TCP software layer of that server divides the sequence of file octets into segments and forwards them individually to the IP software layer (Internet Layer). The Internet Layer encapsulates each TCP segment into an IP packet by adding a header that includes (among other data) the destination IP address. When the client program on the destination computer receives them, the TCP layer (Transport Layer) re-assembles the individual segments and ensures they are correctly ordered and error-free as it streams them to an application.

## HYPERTEXT TRANSFER PROTOCOL

The **Hypertext Transfer Protocol** (**HTTP**) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

Development of HTTP was initiated by Tim Berners-Lee at CERN in 1989. Standards development of HTTP was coordinated by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), culminating in the publication of a series of Requests for Comments (RFCs). The first definition of HTTP/1.1, the version of HTTP in common use, occurred in RFC 2068 in 1997, although this was obsoleted by RFC 2616 in 1999.

A later version, the successor HTTP/2, was standardized in 2015, and is now supported by major web servers.

## Technical Overview




URL beginning with the HTTP scheme and the WWW domain name label.

HTTP functions as a request–response protocol in the client–server computing model. A web browser, for example, may be the client and an application running on a computer hosting a website may be the server. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body.

A web browser is an example of a user agent (UA). Other types of user agent include the indexing software used by search providers (web crawlers), voice browsers, mobile apps, and other software that accesses, consumes, or displays web content.

HTTP is designed to permit intermediate network elements to improve or enable communications between clients and servers. High-traffic websites often benefit from web cache servers that deliver content on behalf of upstream servers to improve response time. Web browsers cache previously accessed web resources and reuse them when possible to reduce network traffic. HTTP proxy servers at private network boundaries can facilitate communication for clients without a globally routable address, by relaying messages with external servers.

HTTP is an application layer protocol designed within the framework of the Internet protocol suite. Its definition presumes an underlying and reliable transport layer protocol, and Transmission Control Protocol (TCP) is commonly used. However HTTP can be adapted to use unreliable protocols such as the User Datagram Protocol (UDP), for example in HTTPU and Simple Service Discovery Protocol (SSDP).

HTTP resources are identified and located on the network by Uniform Resource Locators (URLs), using the Uniform Resource Identifiers (URI's) schemes http and https. URIs and hyperlinks in HTML documents form inter-linked hypertext documents.

HTTP/1.1 is a revision of the original HTTP (HTTP/1.0). In HTTP/1.0 a separate connection to the same server is made for every resource request. HTTP/1.1 can reuse a connection multiple times to download images, scripts, stylesheets, etc after the

page has been delivered. HTTP/1.1 communications therefore experience less latency as the establishment of TCP connections presents considerable overhead.



Tim Berners-Lee

The term hypertext was coined by Ted Nelson in 1965 in the Xanadu Project, which was in turn inspired by Vannevar Bush's vision (1930s) of the microfilm-based information retrieval and management "memex" system described in his essay As We May Think (1945). Tim Berners-Lee and his team at CERN are credited with inventing the original HTTP along with HTML and the associated technology for a web server and a text-based web browser. Berners-Lee first proposed the "WorldWideWeb" project in 1989 — now known as the World Wide Web. The first version of the protocol had only one method, namely GET, which would request a page from a server. The response from the server was always an HTML page.

The first documented version of HTTP was **HTTP V0.9** (1991). Dave Raggett led the HTTP Working Group (HTTP WG) in 1995 and wanted to expand the protocol with extended operations, extended negotiation, richer meta-information, tied with a security protocol which became more efficient by adding additional methods and header fields. RFC 1945 officially introduced and recognized HTTP V1.0 in 1996.

The HTTP WG planned to publish new standards in December 1995 and the support for pre-standard HTTP/1.1 based on the then developing RFC 2068 (called HTTP-NG) was rapidly adopted by the major browser developers in early 1996. By March 1996, pre-standard HTTP/1.1 was supported in Arena, Netscape 2.0, Netscape Navigator Gold 2.01, Mosaic 2.7, Lynx 2.5, and in Internet Explorer 2.0. End-user adoption of the new browsers was rapid. In March 1996, one web hosting company reported that over 40% of browsers in use on the Internet were HTTP 1.1 compliant. That same web hosting company reported that by June 1996, 65% of all browsers accessing their servers were HTTP/1.1 compliant. The HTTP/1.1 standard as defined in RFC 2068 was officially released in January 1997. Improvements and updates to the HTTP/1.1 standard were released under RFC 2616 in June 1999.

In 2007, the **HTTPbis Working Group** was formed, in part, to revise and clarify the HTTP/1.1 specification. In June 2014, the WG released an updated six-part specification obsoleting RFC 2616:

- RFC 7230, HTTP/1.1: Message Syntax and Routing

- RFC 7231, HTTP/1.1: Semantics and Content
- RFC 7232, HTTP/1.1: Conditional Requests
- RFC 7233, HTTP/1.1: Range Requests
- RFC 7234, HTTP/1.1: Caching
- RFC 7235, HTTP/1.1: Authentication

HTTP/2 was published as RFC 7540 in May 2015.

### HTTP Session

An HTTP session is a sequence of network request-response transactions. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a server (typically port 80, occasionally port 8080; see List of TCP and UDP port numbers). An HTTP server listening on that port waits for a client's request message. Upon receiving the request, the server sends back a status line, such as "HTTP/1.1 200 OK", and a message of its own. The body of this message is typically the requested resource, although an error message or other information may also be returned.

### HTTP Authentication

HTTP provides multiple authentication schemes such as Basic access authentication and Digest access authentication which operate via a challenge-response mechanism whereby the server identifies and issues a challenge before serving the requested content.

HTTP provides a general framework for access control and authentication, via an extensible set of challenge-response authentication schemes, which can be used by a server to challenge a client request and by a client to provide authentication information.

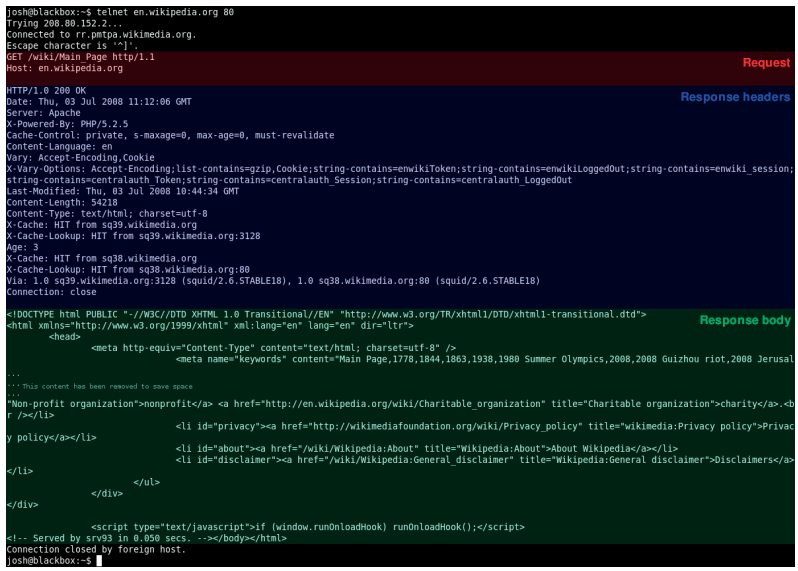
### Authentication Realms

The HTTP Authentication spec also provides an arbitrary, implementation specific construct for further dividing resources common to a given root URI. The realm value string, if present, is combined with the canonical root URI to form the protection space component of the challenge. This in effect allows the server to define separate authentication scopes under one root URI

## Request Methods

HTTP defines methods (sometimes referred to as verbs) to indicate the desired action to be performed on the identified resource. What this resource represents, whether pre-existing data or data that is generated dynamically, depends on the implementation of the server. Often, the resource corresponds to a file or the output of an executable residing on the server. The HTTP/1.0 specification defined the GET, POST and HEAD methods and the HTTP/1.1 specification added 5 new methods: OPTIONS, PUT, DELETE, TRACE and CONNECT. By being specified in these documents their semantics are well known and can be depended on. Any client can use any method and the server can be configured to

support any combination of methods. If a method is unknown to an intermediate it will be treated as an unsafe and non-idempotent method. There is no limit to the number of methods that can be defined and this allows for future methods to be specified without breaking existing infrastructure. For example, WebDAV defined 7 new methods and RFC 5789 specified the PATCH method.




An HTTP 1.1 request made using telnet. The request message, response header section, and response body are highlighted.

## GET

The GET method requests a representation of the specified resource. Requests using GET should only retrieve data and should have no other effect. (This is also true of some other HTTP methods.) The W3C has published guidance principles on this distinction, saying, “Web application design should be informed by the above principles, but also by the relevant limitations.” See safe methods below.

## HEAD

The HEAD method asks for a response identical to that of a GET request, but without the response body. This is useful for retrieving meta-information written in response headers, without having to transport the entire content.

## POST

The POST method requests that the server accept the entity enclosed in the request as a new subordinate of the web resource identified by the URI. The data POSTed might be, for example, an annotation for existing resources; a message for a bulletin board,

newsgroup, mailing list, or comment thread; a block of data that is the result of submitting a web form to a data-handling process; or an item to add to a database.

### PUT

The PUT method requests that the enclosed entity be stored under the supplied URI. If the URI refers to an already existing resource, it is modified; if the URI does not point to an existing resource, then the server can create the resource with that URI.

### DELETE

The DELETE method deletes the specified resource.

### TRACE

The TRACE method echoes the received request so that a client can see what (if any) changes or additions have been made by intermediate servers.

### OPTIONS

The OPTIONS method returns the HTTP methods that the server supports for the specified URL. This can be used to check the functionality of a web server by requesting '*' instead of a specific resource.

### CONNECT

The CONNECT method converts the request connection to a transparent TCP/IP tunnel, usually to facilitate SSL-encrypted communication (HTTPS) through an unencrypted HTTP proxy. See HTTP CONNECT tunneling.

### PATCH

The PATCH method applies partial modifications to a resource.

All general-purpose HTTP servers are required to implement at least the GET and HEAD methods, and, whenever possible, also the OPTIONS method.

### Safe Methods

Some of the methods (for example, HEAD, GET, OPTIONS and TRACE) are, by convention, defined as safe, which means they are intended only for information retrieval and should not change the state of the server. In other words, they should not have side effects, beyond relatively harmless effects such as logging, caching, the serving of banner advertisements or incrementing a web counter. Making arbitrary GET requests without regard to the context of the application's state should therefore be considered safe. However, this is not mandated by the standard, and it is explicitly acknowledged that it cannot be guaranteed.

By contrast, methods such as POST, PUT, DELETE and PATCH are intended for actions that may cause side effects either on the server, or external side effects such as financial transactions or transmission of email. Such methods are therefore not usually used by conforming web robots or web crawlers; some that do not conform tend to make requests without regard to context or consequences.

Despite the prescribed safety of GET requests, in practice their handling by the server is not technically limited in any way. Therefore, careless or deliberate programming can cause non-trivial changes on the server. This is discouraged, because it can cause problems for web caching, search engines and other automated agents, which can make unintended changes on the server.

### *Idempotent Methods and Web Applications*

Methods PUT and DELETE are defined to be idempotent, meaning that multiple identical requests should have the same effect as a single request (note that idempotence refers to the state of the system after the request has completed, so while the action the server takes (e.g. deleting a record) or the response code it returns may be different on subsequent requests, the system state will be the same every time). Methods GET, HEAD, OPTIONS and TRACE, being prescribed as safe, should also be idempotent, as HTTP is a stateless protocol.

In contrast, the POST method is not necessarily idempotent, and therefore sending an identical POST request multiple times may further affect state or cause further side effects (such as financial transactions). In some cases this may be desirable, but in other cases this could be due to an accident, such as when a user does not realize that their action will result in sending another request, or they did not receive adequate feedback that their first request was successful. While web browsers may show alert dialog boxes to warn users in some cases where reloading a page may re-submit a POST request, it is generally up to the web application to handle cases where a POST request should not be submitted more than once.

Note that whether a method is idempotent is not enforced by the protocol or web server. It is perfectly possible to write a web application in which (for example) a database insert or other non-idempotent action is triggered by a GET or other request. Ignoring this recommendation, however, may result in undesirable consequences, if a user agent assumes that repeating the same request is safe when it isn't.

## NETWORK TIME PROTOCOL

Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldest Internet protocols in current use. NTP was designed by David L. Mills of the University of Delaware.

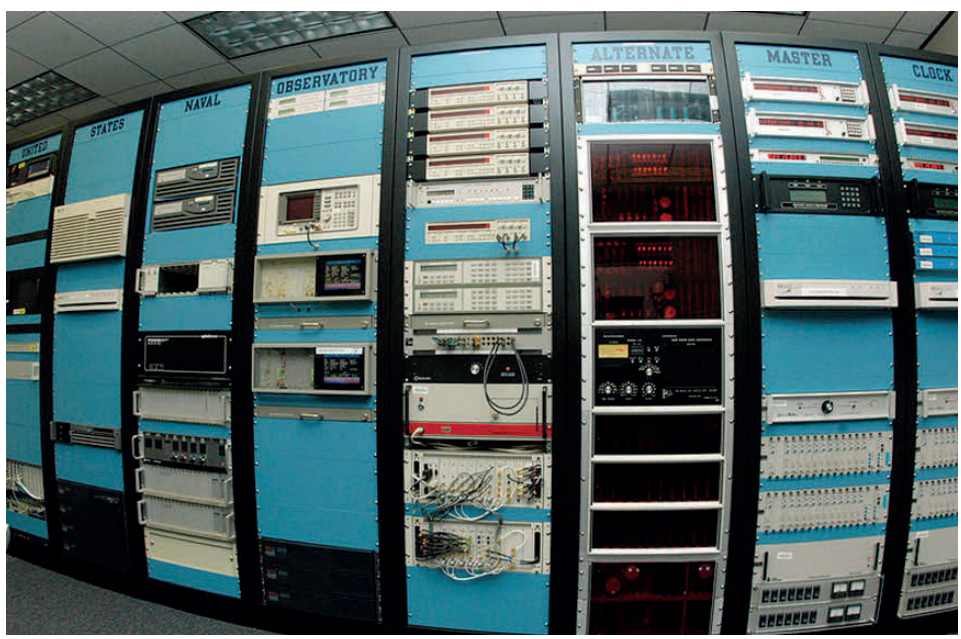
NTP is intended to synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).:3 It uses a modified version of Marzullo's algorithm to select accurate time servers and is designed to mitigate the effects of variable network latency. NTP can usually maintain time to within tens of milliseconds over the public

Internet, and can achieve better than one millisecond accuracy in local area networks under ideal conditions. Asymmetric routes and network congestion can cause errors of 100 ms or more.

The protocol is usually described in terms of a client-server model, but can as easily be used in peer-to-peer relationships where both peers consider the other to be a potential time source.:20 Implementations send and receive timestamps using the User Datagram Protocol (UDP) on port number 123. They can also use broadcasting or multicasting, where clients passively listen to time updates after an initial round-trip calibrating exchange. NTP supplies a warning of any impending leap second adjustment, but no information about local time zones or daylight saving time is transmitted.

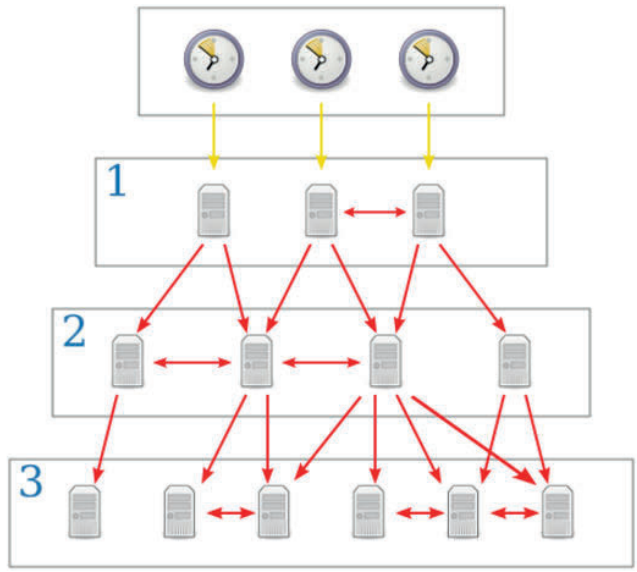
The current protocol is version 4 (NTPv4), which is a proposed standard as documented in RFC 5905. It is backward compatible with version 3, specified in RFC 1305.

## Clock Strata




The U.S. Naval Observatory Alternate Master Clock at Schriever AFB (Colorado) is a stratum 0 source for NTP

NTP uses a hierarchical, semi-layered system of time sources. Each level of this hierarchy is termed a "stratum" and is assigned a number starting with zero at the top. A server synchronized to a stratum n server will be running at stratum n + 1. The number represents the distance from the reference clock and is used to prevent cyclical dependencies in the hierarchy. Stratum is not always an indication of quality or reliability; it is common to find stratum 3 time sources that are higher quality than other stratum 2 time sources. Telecommunication systems use a different definition for clock strata. A brief description of strata 0, 1, 2 and 3 is provided below.




Yellow arrows indicate a direct connection; red arrows indicate a network connection.

## Stratum 0

These are high-precision timekeeping devices such as atomic (cesium, rubidium) clocks, GPS clocks or other radio clocks. They generate a very accurate pulse per second signal that triggers an interrupt and timestamp on a connected computer. Stratum 0 devices are also known as reference clocks.

## Stratum 1

These are computers whose system clocks are synchronized to within a few microseconds of their attached stratum 0 devices. Stratum 1 servers may peer with other stratum 1 servers for sanity checking and backup. They are also referred to as primary time servers.

## Stratum 2

These are computers that are synchronized over a network to stratum 1 servers. Often a stratum 2 computer will query several stratum 1 servers. Stratum 2 computers may also peer with other stratum 2 computers to provide more stable and robust time for all devices in the peer group.

## Stratum 3

These are computers that are synchronized to stratum 2 servers. They employ the same algorithms for peering and data sampling as stratum 2, and can themselves act as servers for stratum 4 computers, and so on.

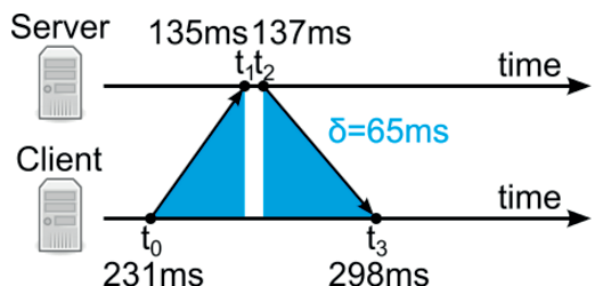
The upper limit for stratum is 15; stratum 16 is used to indicate that a device is unsynchronized. The NTP algorithms on each computer interact to construct a Bellman-Ford shortest-path spanning tree, to minimize the accumulated round-trip delay to the stratum 1 servers for all the clients.

## Timestamps

The 64-bit timestamps used by NTP consist of a 32-bit part for seconds and a 32-bit part for fractional second, giving a time scale that rolls over every $2^{32}$ seconds (136 years) and a theoretical resolution of $2^{-32}$ seconds (233 picoseconds). NTP uses an epoch of January 1, 1900 so the first roll over will be on February 7, 2036.

Future versions of NTP may extend the time representation to 128 bits: 64 bits for the second and 64 bits for the fractional-second. The current NTPv4 format has support for Era Number and Era Offset, that when used properly should aid fixing date rollover issues. According to Mills, "the 64 bit value for the fraction is enough to resolve the amount of time it takes a photon to pass an electron at the speed of light. The 64 bit second value is enough to provide unambiguous time representation until the universe goes dim."

## Clock Synchronization Algorithm




Round-trip delay time δ

A typical NTP client will regularly poll three or more servers on diverse networks. To synchronize its clock, the client must compute their time offset and round-trip delay. Time offset $\theta$ is defined by

$$\theta = \frac{(t_1 - t_0) + (t_2 - t_3)}{2},$$

and the round-trip delay $\delta$ by

$$\delta = (t_3 - t_0) - (t_2 - t_1),$$

where

$t_0$ is the client's timestamp of the request packet transmission,

$t_1$ is the server's timestamp of the request packet reception,

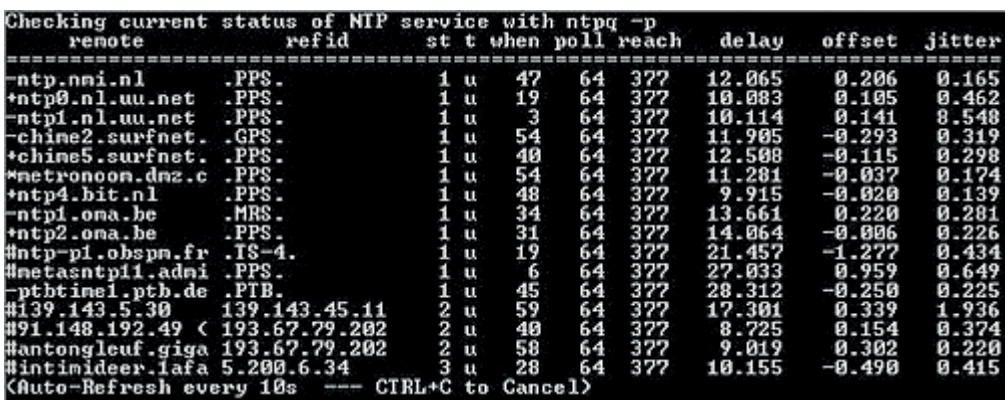
$t_2$ is the server's timestamp of the response packet transmission and

$t_3$ is the client's timestamp of the response packet reception.

The values for $\theta$ and $\delta$ are passed through filters and subjected to statistical analysis. Outliers are discarded and an estimate of time offset is derived from the best three remaining candidates. The clock frequency is then adjusted to reduce the offset gradually, creating a feedback loop.

The synchronization is correct when both the incoming and outgoing routes between the client and the server have symmetrical nominal delay. If the routes do not have a common nominal delay, there will be a systematic bias of half the difference between the forward and backward travel times.

## Software Implementations




The NTP management protocol utility ntpq being used to query the state of a stratum 2 server.

### *Reference Implementation*

The NTP reference implementation, along with the protocol, has been continuously developed for over 20 years. Backwards compatibility has been maintained as new features have been added. It contains several sensitive algorithms, especially to discipline the clock, that can misbehave when synchronized to servers that use different algorithms. The software has been ported to almost every computing platform, including personal computers. It runs as a daemon called ntpd under Unix or as a service under Windows. Reference clocks are supported and their offsets are filtered and analysed in the same way as remote servers, although they are usually polled more frequently.

### *SNTP*

A less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time, is known as the Simple Network Time

Protocol (SNTP). It is used in some embedded devices and in applications where high accuracy timing is not required.

### *Windows Time service*

All Microsoft Windows versions since Windows 2000 include the Windows Time service ("W32Time"), which has the ability to synchronize the computer clock to an NTP server.

The W32Time service was originally implemented for the purpose of the Kerberos version 5 authentication protocol, which required time to be within 5 minutes of the correct value to prevent replay attacks. The version in Windows 2000 and Windows XP only implements Simple NTP, and violates several aspects of the NTP version 3 standard. Beginning with Windows Server 2003 and Windows Vista, a compliant implementation of full NTP is included. Microsoft says that the W32Time service cannot reliably maintain sync time to the range of 1 to 2 seconds. If higher accuracy is desired, Microsoft recommends using a different NTP implementation.

Windows Server 2016 now supports 1 ms time accuracy under the certain operating conditions.

### *Ntimed*

A new NTP client, ntimed, was started by Poul-Henning Kamp in 2014. The new implementation is sponsored by the Linux Foundation as a replacement for the reference implementation, as it was determined to be easier to write a new implementation from scratch than to fix the existing issues with the large existing code base. As of June 2015, no official release was done yet, but ntimed can synchronize clocks reliably. ntimed works under Debian GNU/Linux and FreeBSD, but remains to be ported to Windows and Mac OS.

## REFERENCES

1. "What is Wi-Fi (IEEE 802.11x)? A Webopedia Definition". Webopedia.com.
2. "Brute forcing Wi-Fi Protected Setup" (PDF). Retrieved 2013-06-15.
3. "Authorization of Spread Spectrum Systems Under Parts 15 and 90 of the FCC Rules and Regulations". Federal Communications Commission of the USA. June 18, 1985. Archived from the original(txt) on September 28, 2007. Retrieved 2007-08-31.
4. Ross Greenwood (November 3, 2014). "So just what's the big idea anyway?". News.com.au.
5. Phil Mercer (August 11, 2012). "Wi-fi, dual-flush loos and eight more Australian inventions". BBC News.
6. EP 0599632
7. Sygall, David (December 7, 2009). "How Australia's top scientist earned millions from Wi-Fi". The Sydney Morning Herald.
8. "Wi-Fi Alliance: Organization". Official industry association Web site. Retrieved August 23, 2011.

9. IEEE-SA – IEEE 802.11 and Amendments Patent Letters of Assurance
10. Moses, Asher (June 1, 2010). "CSIRO to reap 'lazy billion' from world's biggest tech companies". The Age. Melbourne. Retrieved 8 June 2010.
11. "World changing Aussie inventions – Australian Geographic". Australian Geographic.
12. "How the Aussie government "invented WiFi" and sued its way to $430 million". Ars Technica.
13. "Australia's Biggest Patent Troll Goes After AT&T, Verizon and T-Mobile". CBS News.
14. "Australian scientists cash in on Wi-Fi invention". The Sydney Morning Herald.
15. "CSIRO wins legal battle over wi-fi patent". ABC News.
16. Sibthorpe, Clare (4 August 2016). "CSIRO Wi-Fi invention to feature in upcoming exhibition at National Museum of Australia". The Canberra Times. Retrieved 4 August 2016.
17. "Statement of Use, s/n 75799629, US Patent and Trademark Office Trademark Status and Document Retrieval". August 23, 2005. Retrieved 2014-09-21. first used the Certification Mark … as early as August 1999
18. "WiFi isn't short for "Wireless Fidelity"". BoingBoing.net. 2005-11-08. Retrieved 2012-12-21.
19. "Wireless Fidelity' Debunked". Wi-Fi Planet. 2007-04-27. Archived from the original on September 28, 2007. Retrieved 2007-08-31.
20. "Securing Wi-Fi Wireless Networks with Today's Technologies"(PDF). Wi-Fi Alliance. February 6, 2003. Retrieved June 25, 2015.
21. "WPA Deployment Guidelines for Public Access Wi-Fi Networks"(PDF). Wi-Fi Alliance. 2004-10-28. Archived from the original (PDF) on March 6, 2007. Retrieved 2009-11-30.
22. https://www.scientificamerican.com/article/pogue-what-wifi-stands-for-other-wireless-questions-answered/
23. HTC S710 User Manual. High Tech Computer Corp. 2006. p. 2. Wi-Fi is a registered trademark of the Wireless Fidelity Alliance, Inc.
24. https://www.ieee.org/about/technologies/emerging/wifi.pdf(originally published 2006)
25. The Wi-Fi Alliance also developed technology that expanded the applicability of Wi-Fi, including a simple set up protocol (Wi-Fi Protected Set Up) and a peer to peer connectivity technology (Wi-Fi Peer to Peer) "Wi-Fi Alliance: Organization". www.wi-fi.org. Retrieved 2009-10-22.
26. "Wi-Fi Alliance: White Papers". www.wi-fi.org. Retrieved 2009-10-22.
27. "Wi-Fi Alliance: Programs". www.wi-fi.org. Retrieved 2009-10-22.
28. "Wi-Fi Alliance". TechTarget. Retrieved 8 April 2016.
29. "Wi-Fi Alliance® statement regarding "Super Wi-Fi"". Wi-Fi Alliance. Retrieved

8 April 2016.

30. Sascha Segan (27 January 2012). "'Super Wi-Fi': Super, But Not Wi-Fi". PC Magazine. Retrieved 8 April 2016.
31. "What Does WiFi Stand For and How Does Wifi Work?". Retrieved November 18, 2015.
32. Marziah Karch (1 September 2010). Android for Work: Productivity for Professionals. Apress. ISBN 978-1-4302-3000-7. Retrieved 11 November 2012.
33. Geier, Jim. "Overview of the IEEE 802.11 Standard". InformIT. Retrieved 8 April 2016.
34. "3.1.1 Packet format" (PDF). IEEE Standard for Ethernet, 802.3-2012 – section one. 2012-12-28. p. 53. Retrieved 2014-07-06.
35. "The Telegraph – Calcutta : Opinion". telegraphindia.com.
36. "Sunnyvale Uses Metro Fi". besttech.com.tr. Archived from the original on July 22, 2015. Retrieved 2008-07-16.
37. Alexander, Steve; Brandt, Steve (December 5, 2010). "Minneapolis moves ahead with wireless". The Star Tribune. Retrieved December 5, 2010.
38. "London-wide wi-fi by 2012 pledge". BBC News. 2010-05-19. Retrieved 2010-05-19.
39. "City of London Fires Up Europe's Most Advanced Wi-Fi Network". www.govtech.com. Retrieved 2007-05-14.
40. Wearden, Graeme (2005-04-18). "London gets a mile of free Wi-Fi". ZDNet. Retrieved 2015-01-06.
41. "Seoul Moves to Provide Free City-Wide WiFi Service". VOANEWS.COM. Retrieved 1 April 2012.
42. Deb Smit (October 5, 2011). "How Wi-Fi got its start on the campus of CMU, a true story". Pop City Media. Retrieved October 6, 2011.
43. "Wireless Andrew: Creating the World's First Wireless Campus". Carnegie Mellon University. 2007. Retrieved October 6, 2011.
44. Wolter Lemstra; Vic Hayes; John Groenewegen (2010). The innovation journey of Wi-Fi: the road to global success. Cambridge University Press. p. 121. ISBN 978-0-521-19971-1. Retrieved October 6, 2011.
45. "Wireless Home Networking with Virtual WiFi Hotspot". Techsansar.com. 2011-01-24. Retrieved 2011-10-14.
46. "Wi-Fi Direct allows device-to-device links".
47. "Wi-Fi gets personal: Groundbreaking Wi-Fi Direct launches today". Wi-Fi Alliance. October 25, 2010. Retrieved June 25, 2015.
48. "What is Wi-Fi Certified TDLS?".
49. Delia C. "WiFi baby monitor security". MonitorsHQ.com. Retrieved 2014-09-12.
50. Wilson, Tracy V. "How Municipal WiFi Works". computer.howstuffworks.com. Retrieved 2008-03-12.

51. Murph, Darren. “Study: 802.11ac devices to hit the one billion mark in 2015, get certified in 2048”. Engadget. Retrieved 25 August 2014.
52. Karan (2016). “Highly Useful Wi-Fi Analyzer Apps For Android and iOS”. FocusAndLeap.com.
53. “Apple.com Airport Utility Product Page”. Apple, Inc. Retrieved 2011-06-14.
54. GainSpan specifically designs for Wi-Fi technology between Wi-Fi devices. Extremely useful. “GainSpan low-power, embedded Wi-Fi”. www.gainspan.com. Retrieved 2010. Check date values in: |access-date= (help)
55. “Quatech Rolls Out Airborne Embedded 802.11 Radio for M2M Market”. Retrieved 2008-04-29.
56. “CIE article on embedded Wi-Fi for M2M applications”. Retrieved 2014-11-28.
57. “Somebody explain dBi – Wireless Networking – DSLReports Forums”. DSL Reports.
58. “802.11n Delivers Better Range”. Wi-Fi Planet. 2007-05-31. Archived from the original on November 8, 2015.
59. section 1.2 (scope)
60. Muller, Scott. Upgrading and Reparing PCs (22nd ed.). Pearson Education. p. 898. ISBN 978-0-7897-5610-7.
61. “WiFi Mapping Software:Footprint”. Alyrica Networks. Retrieved 2008-04-27.
62. “Ermanno Pietrosemoli has set a new record for the longest communication Wi-Fi link”. Retrieved 2008-03-10.
63. “Wireless technology is irreplaceable for providing access in remote and scarcely populated regions”. Retrieved 2008-03-10.
64. “Long Distance WiFi Trial” (PDF). Retrieved 2008-03-10.
65. “802.11 X Wireless Network in a Business Environment – Pros and Cons.”. NetworkBits.net. Retrieved 2008-04-08.
66. “Free Wi-Fi? User beware: Open connections to Internet are full of security dangers, hackers, ID thieves”. Larry Higgs – Asbury Park Press.
67. Gittleson, Kim (28 March 2014) Data-stealing Snoopy drone unveiled at Black Hat BBC News, Technology, Retrieved 29 March 2014
68. Bernstein, Daniel J. (2002). “DNS forgery”. Retrieved 2010-03-24. An attacker with access to your network can easily forge responses to your computer’s DNS requests.
69. Mateti, Prabhaker (2005). “Hacking Techniques in Wireless Networks”. Dayton, Ohio: Department of Computer Science and Engineering Wright State University. Retrieved 2010-02-28.
70. “Wireless Vulnerabilities & Exploits”. wirelessve.org. Retrieved 2008-04-15.
71. “WPA2 Security Now Mandatory for Wi-Fi CERTIFIED Products” “WPA2 Security Now Mandatory for Wi-Fi CERTIFIED Products”. Wi-Fi Alliance.

72. http://www.kb.cert.org/vuls/id/723755 US CERT Vulnerability Note VU#723755
73. "NoCat's goal is to bring you Infinite Bandwidth Everywhere for Free". Nocat.net. Retrieved 2011-10-14.
74. "Let's Warchalk" (PDF). Matt Jones. Retrieved 2008-10-09.
75. "Electromagnetic fields and public health - Base stations and wireless technologies". World Health Organization. 2006. Retrieved 2016-05-28.
76. "IARC Classifies Radiofrequency Electromagnetic Fields as Possibly Carcinogenic to Humans" (pdf). International Agency for Research on Cancer. 2011. Retrieved 2016-05-28.
77. "Electromagnetic Fields and Public Health: Mobile Phones". World Health Organization. October 2014. Retrieved 2016-05-28.
78. "Q&A: Wi-fi health concerns". BBC News. 2007-05-21. Retrieved 2016-05-28.
79. Rubin, GJ; Das Munshi, J; Wessely, S (2005-03-01). "Electromagnetic Hypersensitivity: A Systematic Review of Provocation Studies". Psychosom Med. 67: 224–32. doi:10.1097/01.psy.0000155664.13300.64. PMID 15784787.
80. Forouzan, B.A. (2000). TCP/IP: Protocol Suite (1st ed.). New Delhi, India: Tata McGraw-Hill Publishing Company Limited.
81. Kozierok, Charles M. (2005). "The TCP/IP Guide v3.0". Tcpipguide.com.
82. Dean, Tamara (2010). Network+ Guide to Networks. Delmar. pp. 168–171.
83. Clark, M.P. (2003). Data Networks IP and the Internet (1st ed.). West Sussex, England: John Wiley & Sons Ltd.
84. "Active FTP vs. Passive FTP, a Definitive Explanation". Slacksite.com. Archived from the original on 2014-12-31.
85. Parker, Don (September 2005). "Understanding the FTP Protocol". Windowsnetworking.com.
86. RFC 959 (Standard) File Transfer Protocol (FTP). Postel, J. & Reynolds, J. (October 1985).
87. RFC 2428 (Proposed Standard) Extensions for IPv6, NAT, and Extended Passive Mode. Allman, M. & Metz, C. & Ostermann, S. (September 1998).
88. Preston, J. (January 2005). Deflate transmission mode for FTP. IETF. I-D draft-preston-ftpext-deflate-03.txt. Retrieved 27 January 2016.
89. RFC 1635 (Informational) How to Use Anonymous FTP. P. & Emtage, A. & Marine, A. (May 1994).
90. Gleason, Mike (2005). "The File Transfer Protocol and Your Firewall/NAT". Ncftp.com.
91. Matthews, J. (2005). Computer Networking: Internet Protocols in Action (1st ed.). Danvers, MA: John Wiley & Sons Inc.
92. "Accessing FTP servers | How to | Firefox Help". Support.mozilla.com. 2012-09-05. Retrieved 2013-01-16.
93. "How to Enter FTP Site Password in Internet Explorer". Support.microsoft.com.

2011-09-23. Retrieved 2015-03-28. Written for IE versions 6 and earlier. Might work with newer versions.

94. "Securing FTP using SSH". Nurdletech.com.
95. http://ssh.com/index.php/products/tectia-pci-point-to-point-encryption.html
96. Vinton G. Cerf; Robert E. Kahn (May 1974). "A Protocol for Packet Network Intercommunication" (PDF). IEEE Transactions on Communications. 22 (5): 637–648. doi:10.1109/tcom.1974.1092259. Archived from the original (PDF) on March 4, 2016.
97. Comer, Douglas E. (2006). Internetworking with TCP/IP:Principles, Protocols, and Architecture. 1 (5th ed.). Prentice Hall. ISBN 0-13-187671-6.
98. "TCP (Linktionary term)".
99. "RFC 791 – section 2.1".
100. "RFC 793".
101. "RFC 1323, TCP Extensions for High Performance, Section 2.2".
102. "RFC 2018, TCP Selective Acknowledgement Options, Section 2".
103. "RFC 2018, TCP Selective Acknowledgement Options, Section 3".
104. "RFC 1323, TCP Extensions for High Performance, Section 3.2".
105. RFC 793 section 3.1
106. RFC 793 Section 3.2
107. Tanenbaum, Andrew S. (2003-03-17). Computer Networks (Fourth ed.). Prentice Hall. ISBN 0-13-066102-3.
108. "TCP Definition". Retrieved 2011-03-12.
109. Mathis; Mathew; Semke; Mahdavi; Ott (1997). "The macroscopic behavior of the TCP congestion avoidance algorithm". ACM SIGCOMM Computer Communication Review. 27.3: 67–82.
110. Paxson, V.; Allman, M.; Chu, J.; Sargent, M. (June 2011). "The Basic Algorithm". Computing TCP's Retransmission Timer. IETF. p. 2. sec. 2. RFC 6298. Retrieved October 24, 2015.
111. Stone; Partridge (2000). "When The CRC and TCP Checksum Disagree". Sigcomm.
112. "RFC 879".
113. "TCP window scaling and broken routers [LWN.net]".
114. Gont, Fernando (November 2008). "On the implementation of TCP urgent data". 73rd IETF meeting. Retrieved 2009-01-04.
115. Peterson, Larry (2003). Computer Networks. Morgan Kaufmann. p. 401. ISBN 1-55860-832-X.
116. Richard W. Stevens (2006). November 2011 TCP/IP Illustrated. Vol. 1, The protocols Check |url= value (help). Addison-Wesley. pp. Chapter 20. ISBN 978-0-201-63346-7.

117. Security Assessment of the Transmission Control Protocol (TCP) at the Wayback Machine (archived March 6, 2009)
118. Security Assessment of the Transmission Control Protocol (TCP)
119. Jakob Lell. "Quick Blind TCP Connection Spoofing with SYN Cookies". Retrieved 2014-02-05.
120. Some insights about the recent TCP DoS (Denial of Service) vulnerabilities
121. "Exploiting TCP and the Persist Timer Infiniteness".
122. "Laurent Joncheray, Simple Active Attack Against TCP, 1995".
123. John T. Hagen; Barry E. Mullins (2013). "TCP veto: A novel network attack and its application to SCADA protocols". Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES.
124. TCP Interactive (iTCP)
125. RFC 6182
126. RFC 6824
127. "TCP with feed-forward source coding for wireless downlink networks".
128. Raiciu; Barre; Pluntke; Greenhalgh; Wischik; Handley (2011). "Improving datacenter performance and robustness with multipath TCP". Sigcomm.
129. "MultiPath TCP - Linux Kernel implementation".
130. Barre; Paasch; Bonaventure (2011). "MultiPath TCP: From Theory to Practice". IFIP Networking.
131. Raiciu; Paasch; Barre; Ford; Honda; Duchene; Bonaventure; Handley (2012). "How Hard Can It Be? Designing and Implementing a Deployable Multipath TCP". USENIX NSDI.
132. Michael Kerrisk (2012-08-01). "TCP Fast Open: expediting web services". LWN.net.
133. Y. Cheng, J. Chu, S. Radhakrishnan, A. Jain (2012-07-16). TCP Fast Open. IETF. I-D draft-ietf-tcpm-fastopen-01.
134. "RFC 6937 - Proportional Rate Reduction for TCP". http://tools.ietf.org/html/rfc6937. External link in |website= (help);
135. Grigorik, Ilya (2013). High-performance browser networking (1. ed.). Beijing: O'Reilly. ISBN 1449344763.
136. "TCP performance over CDMA2000 RLP". Retrieved 2010-08-30
137. Muhammad Adeel & Ahmad Ali Iqbal (2004). "TCP Congestion Window Optimization for CDMA2000 Packet Data Networks". International Conference on Information Technology (ITNG'07): 31–35. doi:10.1109/ITNG.2007.190. ISBN 978-0-7695-2776-5.
138. Yunhong Gu, Xinwei Hong, and Robert L. Grossman. "An Analysis of AIMD Algorithm with Decreasing Increases". 2004.
139. Fielding, Roy T.; Gettys, James; Mogul, Jeffrey C.; Nielsen, Henrik Frystyk; Masinter, Larry; Leach, Paul J.; Berners-Lee, Tim (June 1999). Hypertext

Transfer Protocol -- HTTP/1.1. IETF. RFC 2616.

140. "Overall Operation". p. 12. sec. 1.4. RFC 2616.
141. Berners-Lee, Tim. "HyperText Transfer Protocol". World Wide Web Consortium. Retrieved 31 August 2010.
142. Tim Berners-Lee. "The Original HTTP as defined in 1991". World Wide Web Consortium. Retrieved 24 July 2010.
143. Raggett, Dave. "Dave Raggett's Bio". World Wide Web Consortium. Retrieved 11 June 2010.
144. Raggett, Dave; Berners-Lee, Tim. "Hypertext Transfer Protocol Working Group". World Wide Web Consortium. Retrieved 29 September 2010.
145. Raggett, Dave. "HTTP WG Plans". World Wide Web Consortium. Retrieved 29 September 2010.
146. Simon Spero. "Progress on HTTP-NG". World Wide Web Consortium. Retrieved 11 June 2010.
147. "HTTP/1.1". Webcom.com Glossary entry. Retrieved 2009-05-29.
148. Fielding, Roy T.; Reschke, Julian F. (June 2014). Hypertext Transfer Protocol (HTTP/1.1): Authentication. IETF. RFC 7235.
149. Berners-Lee, Tim; Fielding, Roy T.; Nielsen, Henrik Frystyk. "Method Definitions". Hypertext Transfer Protocol -- HTTP/1.0. IETF. pp. 30-32. sec. 8. RFC 1945.
150. "Method Definitions". pp. 51-57. sec. 9. RFC 2616.
151. Jacobs, Ian (2004). "URIs, Addressability, and the use of HTTP GET and POST". Technical Architecture Group finding. W3C. Retrieved 26 September 2010.
152. "POST". p. 54. sec. 9.5. RFC 2616.
153. "PUT". p. 55. sec. 9.6. RFC 2616.
154. "CONNECT". Hypertext Transfer Protocol -- HTTP/1.1. IETF. June 1999. p. 57. sec. 9.9. RFC 2616. Retrieved 23 February 2014.
155. Khare, Rohit; Lawrence, Scott (May 2000). Upgrading to TLS Within HTTP/1.1. IETF. RFC 2817.
156. "Vulnerability Note VU#150227: HTTP proxy default configurations allow arbitrary TCP connections". US-CERT. 2002-05-17. Retrieved 2007-05-10.
157. Dusseault, Lisa; Snell, James M. (March 2010). PATCH Method for HTTP. IETF. RFC 5789.
158. "Method". p. 36. sec. 5.1.1. RFC 2616.
159. "Cross Site Tracing". OWASP. Retrieved 2016-06-22.
160. "Status-Line". p. 39. sec. 6.1. RFC 2616.
161. Canavan, John (2001). Fundamentals of Networking Security. Norwood, MA: Artech House. pp. 82–83. ISBN 9781580531764.
162. Zalewski, Michal. "Browser Security Handbook". Retrieved 30 April 2015.

163. "Chromium Issue 4527: implement RFC 2817: Upgrading to TLS Within HTTP/1.1". Retrieved 30 April 2015.
164. "Mozilla Bug 276813 - [RFE] Support RFC 2817 / TLS Upgrade for HTTP 1.1". Retrieved 30 April 2015.
165. "HTTP Message". p. 31. sec. 4. RFC 2616.
166. "Apache Week. HTTP/1.1". 090502 apacheweek.com
167. "Canonicalization and Text Defaults". sec. 3.7.1. RFC 2616.
168. Luotonen, Ari; Franks, John (February 22, 1996). Byte Range Retrieval Extension to HTTP. IETF. I-D draft-ietf-http-range-retrieval-00.
169. Nottingham, Mark (October 2010). Web Linking. IETF. RFC 5988.
170. "Hypertext Transfer Protocol Bis (httpbis) – Charter". IETF. 2012.
171. David L. Mills (12 December 2010). Computer Network Time Synchronization: The Network Time Protocol. Taylor & Francis. pp. 12–. ISBN 978-0-8493-5805-0.
172. "Executive Summary: Computer Network Time Synchronization". Retrieved 2011-11-21.
173. "NTP FAQ". The NTP Project. Retrieved 2011-08-27.
174. "Port Numbers". The Internet Assigned Numbers Authority (IANA).
175. Page 16
176. David L. Mills (15 November 2010). Computer Network Time Synchronization: The Network Time Protocol on Earth and in Space, Second Edition. CRC Press. p. 377. ISBN 978-1-4398-1464-2.
177. "Network Time Synchronization Research Project". Retrieved 24 December 2014.
178. "NTP Needs Money: Is A Foundation The Answer?". InformationWeek. March 23, 2015. Retrieved April 4, 2015.
179. "NTP's Fate Hinges On 'Father Time'". InformationWeek. March 11, 2015. Retrieved April 4, 2015.
180. "Network Time Protocol: Best Practices White Paper". Retrieved 15 October 2013.
181. David L. Mills (12 May 2012). "The NTP Era and Era Numbering". Retrieved 24 September 2016.
182. W. Richard Stevens; Bill Fenner; Andrew M. Rudoff (2004). UNIX Network Programming. Addison-Wesley Professional. pp. 582–. ISBN 978-0-13-141155-5.
183. University of Delaware Digital Systems Seminar presentation by David Mills, 2006-04-26
184. Gotoh, T.; Imamura, K.; Kaneko, A. (2002). Improvement of NTP time offset under the asymmetric network with double packets method. Conference on Precision Electromagnetic Measurements. pp. 448–449. doi:10.1109/CPEM.2002.1034915. ISBN 0-7803-7242-5.
185. "Network Time Protocol Version 4: Protocol and Algorithms Specification". June 2010. p. 54. Retrieved 2012-08-26. Primary servers and clients complying with a subset of NTP, called the Simple Network Time Protocol (SNTPv4) [...], do

not need to implement the mitigation algorithms [...] The fully developed NTPv4 implementation is intended for [...] servers with multiple upstream servers and multiple downstream servers [...] Other than these considerations, NTP and SNTP servers and clients are completely interoperable and can be intermixed [...]

186. RFC 4330
187. RFC 5905
188. "Windows Time Service Technical Reference". technet.microsoft.com. 2011-08-17. Retrieved 2011-09-19.
189. "Windows Time Service page at NTP.org". Support.ntp.org. 2008-02-25. Retrieved 2011-01-12.
190. "How the Windows Time Service Works". technet.microsoft.com. 2010-03-12. Retrieved 2011-09-19.
191. "Support boundary to configure the Windows Time service for high accuracy environments". Microsoft Corporation. 2011-10-19.
192. Ned Pyle (2007-10-23). "High Accuracy W32time Requirements". Microsoft Corporation. Retrieved 2012-08-26.
193. https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/get-started/windows-time-service/windows-2016-accurate-time
194. Poul-Henning, Kamp. "20140926 – Playing with time again". PHK's Bikeshed. Retrieved 4 June 2015.
195. Poul-Henning, Kamp. "Network time synchronization software, NTPD replacement.". ntimed git repository README file. Github. Retrieved 4 June 2015.
196. Poul-Henning, Kamp (2015-01-11). "20150111 – What happened next?". PHK's Bikeshed. Retrieved 4 June 2015.
197. David Mills. "The NTP Timescale and Leap Seconds". Retrieved 15 October 2013.
198. "Network Time Protocol Version 4: Autokey Specification". IETF. 2010. Retrieved 2014-10-16.
199. "NTP Security Analysis". Retrieved 11 October 2013.
200. Jose Selvi (2014-10-16). "Bypassing HTTP Strict Transport Security" (PDF). Retrieved 2014-10-16.
201. Aanchal Malhotra; Isaac E. Cohen; Erik Brakke & Sharon Goldberg (20 October 2015). "Attacking the Network Time Protocol" (PDF). NDSS.
202. "Attacking the Network Time Protocol". www.cs.bu.edu. Retrieved 2015-10-27.
203. "Security Notice". Support.ntp.org. 2009-12-10. Retrieved 2011-01-12.
204. results returned by a search on "Network Time Protocol" at [original research?]
205. in RFC 778, RFC 891, RFC 956, RFC 958, RFC 1305, RFC 5905, and the NTPv4 specification

206. “Code Audit”. Support.ntp.org. 2009-06-13. Retrieved 2011-01-12.
207. Goodin, Dan (2014-01-13). “New DoS attacks taking down game sites deliver crippling 100Gbps floods”. Ars Technica. Retrieved 2014-01-25.
208. Lee, Dave (2014-02-11). “Huge hack ‘ugly sign of future’ for internet threats”. BBC. Retrieved 2014-02-12.
209. “DRDoS / Amplification Attack using ntpdc monlist command”. support.ntp.org. 2010-04-24. Retrieved 2014-04-13.
210. “Network Time Protocol Vulnerabilities (Update C) | ICS-CERT”. Ics-cert.us-cert.gov. Retrieved 2015-04-15.
211. Cunningham, Andrew (Dec 23, 2014). “Apple automatically patches Macs to fix severe NTP security flaw”. arstechnica. Retrieved Apr 29, 2015.
212. “NTP vulnerability on versions prior to 4.2.8 -- we OK?”. Apple Support Communities.
213. Fairhead, Harry (23 December 2014). “NTP The Latest Open Source Security Problem”. I Programmer.

CHAPTER 6

# Ethernet

## Chapter Contents

- **Introduction**
- **Autonegotiation**

Ethernet is a standard communications protocol embedded in software and hardware devices, intended for building a local area network (LAN). It was designed by Bob Metcalfe in 1973, and through the efforts of Digital, Intel and Xerox (for which Metcalfe worked), "DIX" Ethernet became the standard model for LANs worldwide.

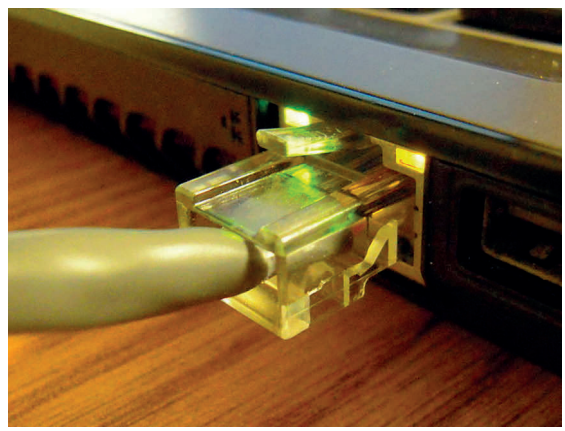
## INTRODUCTION

Ethernet is a family of computer networking technologies commonly used in local area networks (LANs) and metropolitan area networks (MANs). It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3, and has since been refined to support higher bit rates and longer link distances. Over time, Ethernet has largely replaced competing wired LAN technologies such as token ring, FDDI and ARCNET.

The original 10BASE5 Ethernet uses coaxial cable as a shared medium, while the newer Ethernet variants use twisted pair and fiber optic links in conjunction with hubs or switches. Over the course of its history, Ethernet data transfer rates have been increased from the original 2.94 megabits per second (Mbit/s) to the latest 100 gigabits per second (Gbit/s). The Ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet.

Systems communicating over Ethernet divide a stream of data into shorter pieces called frames. Each frame contains source and destination addresses, and error-checking data so that damaged frames can be detected and discarded; most often, higher-layer protocols trigger retransmission of lost frames. As per the OSI model, Ethernet provides services up to and including the data link layer.

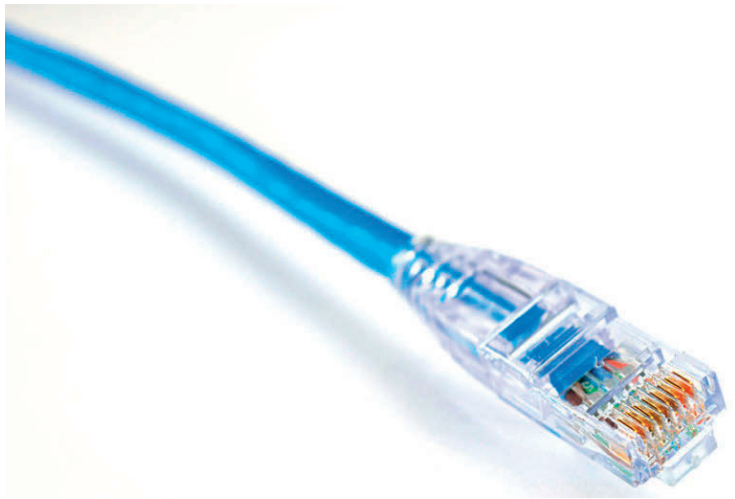
Since its commercial release, Ethernet has retained a good degree of backward compatibility. Features such as the 48-bit MAC address and Ethernet frame format have influenced other networking protocols. The primary alternative for some uses of contemporary LANs is Wi-Fi, a wireless protocol standardized as IEEE 802.11.



A Cat 5e connection on a laptop, used for Ethernet

Ethernet was developed at Xerox PARC between 1973 and 1974. It was inspired by ALOHAnet, which Robert Metcalfe had studied as part of his PhD dissertation. The idea was first documented in a memo that Metcalfe wrote on May 22, 1973, where he named it after the disproven luminiferous ether as an "omnipresent, completely-passive medium for the propagation of electromagnetic waves". In 1975, Xerox filed a patent application listing Metcalfe, David Boggs, Chuck Thacker, and Butler Lampson as inventors. In 1976, after the system was deployed at PARC, Metcalfe and Boggs published a seminal paper.

Metcalfe left Xerox in June 1979 to form 3Com. He convinced Digital Equipment Corporation (DEC), Intel, and Xerox to work together to promote Ethernet as a standard. The so-called "DIX" standard, for "Digital/Intel/Xerox", specified 10 Mbit/s Ethernet, with 48-bit destination and source addresses and a global 16-bit Ethertype-type field. It was published on September 30, 1980 as "The Ethernet, A Local Area Network. Data Link Layer and Physical Layer Specifications". Version 2 was published in November, 1982 and defines what has become known as Ethernet II. Formal standardization efforts proceeded at the same time and resulted in the publication of IEEE 802.3 on June 23, 1983.

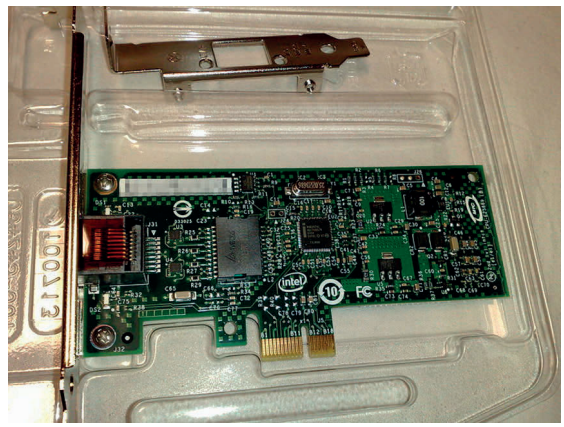


An 8P8C modular connector (often called RJ45) commonly used on Cat 5 cables in Ethernet networks

Ethernet initially competed with two largely proprietary systems, Token Ring and Token Bus. Because Ethernet was able to adapt to market realities and shift to inexpensive and ubiquitous twisted pair wiring, these proprietary protocols soon found themselves competing in a market inundated by Ethernet products, and, by the end of the 1980s, Ethernet was clearly the dominant network technology. In the process, 3Com became a major company. 3Com shipped its first 10 Mbit/s Ethernet 3C100 NIC in March 1981, and that year started selling adapters for PDP-11s and VAXes, as well as Multibus-based Intel and Sun Microsystems computers.[9] This was followed quickly by DEC's Unibus to Ethernet adapter, which DEC sold and used internally to build its own corporate network, which reached over 10,000 nodes by 1986, making it one of the largest computer networks in the world at that time. An Ethernet adapter card for the IBM PC was released in 1982, and, by 1985, 3Com had sold 100,000. By the early 1990s, Ethernet became so prevalent that it was a must-have feature for modern computers, and Ethernet ports began to appear on some PCs and most workstations. This process was greatly sped up with the introduction of 10BASE-T and its relatively small modular connector, at which point Ethernet ports appeared even on low-end motherboards.

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

## Standardization



An Intel 82574L Gigabit Ethernet NIC, PCI Express x1 card

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

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

Approval of Ethernet on the international level was achieved by a similar, cross-partisan action with Fromm as the liaison officer working to integrate with International Electrotechnical Commission (IEC) Technical Committee 83 (TC83) and International Organization for Standardization (ISO) Technical Committee 97 Sub Committee 6 (TC97SC6). The ISO 8802-3 standard was published in 1989.

## Evolution

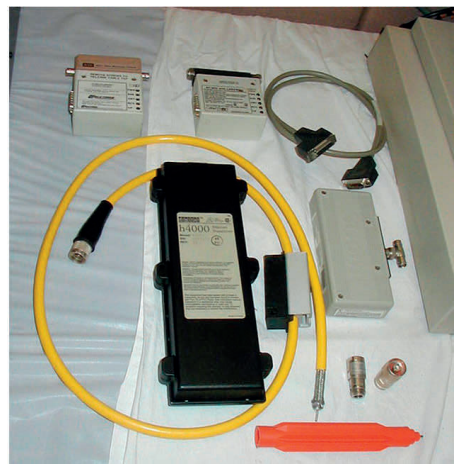
Ethernet evolved to include higher bandwidth, improved media access control methods, and different physical media. The coaxial cable was replaced with point-to-point links connected by Ethernet repeaters or switches.

Ethernet stations communicate by sending each other data packets: blocks of data individually sent and delivered. As with other IEEE 802 LANs, each Ethernet station is given a 48-bit MAC address. The MAC addresses are used to specify both the destination and the source of each data packet. Ethernet establishes link level connections, which can be defined using both the destination and source addresses. On reception of a transmission, the receiver uses the destination address to determine whether the transmission is relevant to the station or should be ignored. Network interfaces normally do not accept packets addressed to other Ethernet stations. Adapters come programmed with a globally unique address.

An EtherType field in each frame is used by the operating system on the receiving station to select the appropriate protocol module (e.g., an Internet Protocol version such as IPv4). Ethernet frames are said to be *self-identifying*, because of the frame type. Self-identifying frames make it possible to intermix multiple protocols on the same physical network and allow a single computer to use multiple protocols together. Despite the evolution of Ethernet technology, all generations of Ethernet (excluding early experimental versions) use the same frame formats. Mixed-speed networks can be built using Ethernet switches and repeaters supporting the desired Ethernet variants.

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

### *Shared Media*



Older Ethernet equipment. Clockwise from top-left: An Ethernet transceiver with an in-line 10BASE2 adapter, a similar model transceiver with a 10BASE5 adapter, an AUI

cable, a different style of transceiver with 10BASE2 BNC T-connector, two 10BASE5 end fittings (N connectors), an orange "vampire tap" installation tool (which includes a specialized drill bit at one end and a socket wrench at the other), and an early model 10BASE5 transceiver (h4000) manufactured by DEC. The short length of yellow 10BASE5 cable has one end fitted with a N connector and the other end prepared to have a N connector shell installed; the half-black, half-grey rectangular object through which the cable passes is an installed vampire tap.

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

Original Ethernet's shared coaxial cable (the shared medium) traversed a building or campus to every attached machine. A scheme known as carrier sense multiple access with collision detection (CSMA/CD) governed the way the computers shared the channel. This scheme was simpler than the competing token ring or token bus technologies.[d] Computers are connected to an Attachment Unit Interface (AUI) transceiver, which is in turn connected to the cable (with thin Ethernet the transceiver is integrated into the network adapter). While a simple passive wire is highly reliable for small networks, it is not reliable for large extended networks, where damage to the wire in a single place, or a single bad connector, can make the whole Ethernet segment unusable.[e]

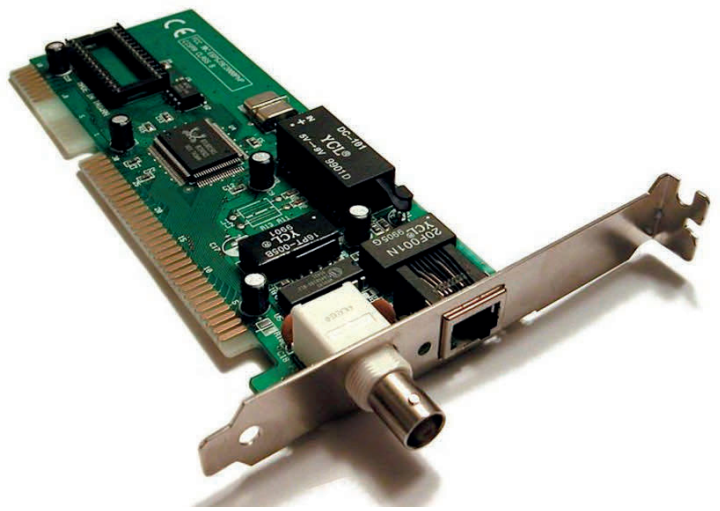
Through the first half of the 1980s, Ethernet's 10BASE5 implementation used a coaxial cable 0.375 inches (9.5 mm) in diameter, later called "thick Ethernet" or "thicknet". Its successor, 10BASE2, called "thin Ethernet" or "thinnet", used the RG-58 coaxial cable. The emphasis was on making installation of the cable easier and less costly.:57

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

Collisions happen when two stations attempt to transmit at the same time. They corrupt transmitted data and require stations to retransmit. The lost data and retransmissions reduce throughput. In the worst case where multiple active hosts connected with maximum allowed cable length attempt to transmit many short frames, excessive collisions can reduce throughput dramatically. However, a Xerox report in 1980 studied performance of an existing Ethernet installation under both normal and artificially generated heavy load. The report claims that 98% throughput on the LAN was observed. This is in contrast with token passing LANs (token ring, token bus), all of which suffer throughput degradation as each new node comes into the LAN, due to token waits. This report was controversial, as modeling showed that collision-based networks theoretically became unstable under loads as low as 37% of nominal capacity. Many early researchers failed to understand these results. Performance on real networks is significantly better.

In a modern Ethernet, the stations do not all share one channel through a shared cable or a simple repeater hub; instead, each station communicates with a switch, which in turn forwards that traffic to the destination station. In this topology, collisions are only possible if station and switch attempt to communicate with each other at the same time, and collisions are limited to this link. Furthermore, the 10BASE-T standard introduced a full duplex mode of operation which has become extremely common. In full duplex, switch and station can communicate with each other simultaneously, and therefore modern Ethernets are completely collision-free.

## Repeaters and Hubs



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

## Main article: Ethernet hub

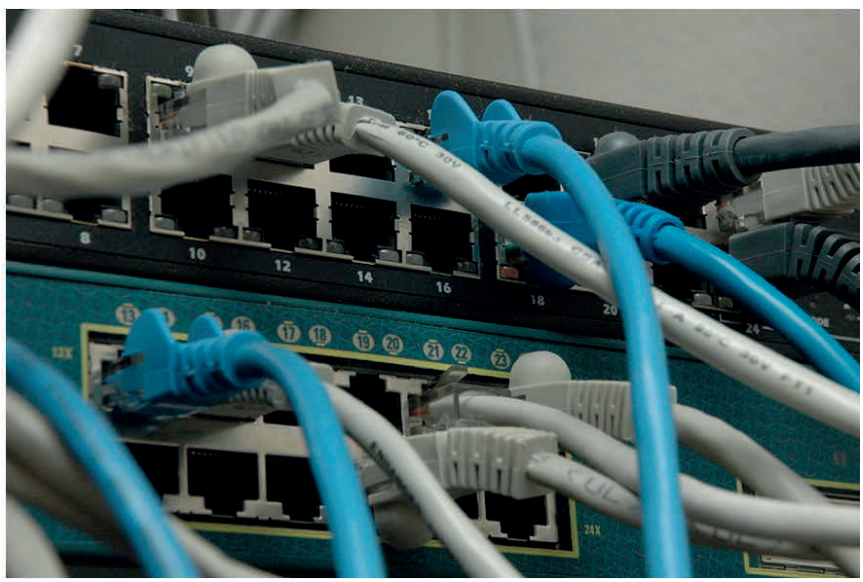
For signal degradation and timing reasons, coaxial Ethernet segments have a restricted size. Somewhat larger networks can be built by using an Ethernet repeater. Early repeaters had only two ports, allowing, at most, a doubling of network size. Once repeaters with more than two ports became available,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

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

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

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

## *Bridging and Switching*



Patch cables with patch fields of two Ethernet switches

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

To alleviate these problems, bridging was created to communicate at the data link layer while isolating the physical layer. With bridging, only well-formed Ethernet packets are forwarded from one Ethernet segment to another; collisions and packet errors are isolated. At initial startup, Ethernet bridges (and switches) work somewhat like Ethernet repeaters, passing all traffic between segments. By observing the source addresses of incoming frames, the bridge then builds an address table associating addresses to segments. Once an address is learned, the bridge forwards network traffic destined for that address only to the associated segment, improving overall performance. Broadcast traffic is still forwarded to all network segments. Bridges also overcome the limits on total segments between two hosts and allow the mixing of speeds, both of which are critical to deployment of Fast Ethernet.

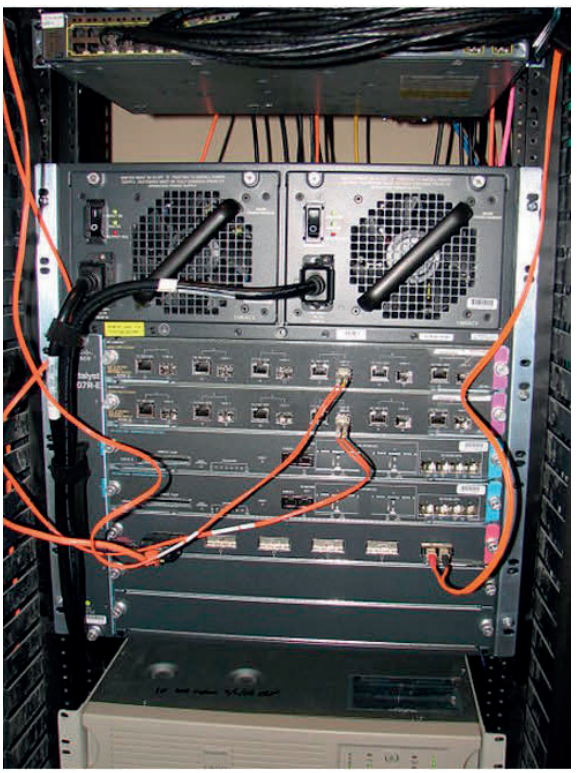
In 1989, the networking company Kalpana (acquired by Cisco Systems, Inc. in 1994) introduced their EtherSwitch, the first Ethernet switch.[h] This works somewhat differently from an Ethernet bridge, where only the header of the incoming packet is examined before it is either dropped or forwarded to another segment. This greatly reduces the forwarding latency and the processing load on the network device. One drawback of this cut-through switching method is that packets that have been corrupted are still propagated through the network, so a jabbering station can continue to disrupt the entire network. The eventual remedy for this was a return to the original store and forward approach of bridging, where the packet would be read into a buffer on the switch in its entirety, verified against its checksum and then forwarded, but using more powerful application-specific integrated circuits. Hence, the bridging is then done in hardware, allowing packets to be forwarded at full wire speed.

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

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

The bandwidth advantages, the improved isolation of devices from each other, the ability to easily mix different speeds of devices and the elimination of the chaining limits inherent in non-switched Ethernet have made switched Ethernet the dominant network technology.

## Advanced Networking



A core Ethernet switch

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

Advanced networking features in switches and routers use shortest path bridging and spanning-tree protocol, for example, to maintain the active links of the network as a tree while allowing physical loops for redundancy, ensure port security and protection features such as MAC lockdown and broadcast radiation filtering, use virtual LANs to keep different classes of users separate while using the same physical infrastructure, employ multilayer switching to route between different classes, and use link aggregation to add bandwidth to overloaded links and to provide some redundancy.

IEEE 802.1aq (shortest path bridging) includes the use of the link-state routing protocol IS-IS to allow larger networks with shortest path routes between devices. In 2012, it was stated by David Allan and Nigel Bragg, in *802.1aq Shortest Path Bridging Design and Evolution: The Architect's Perspective* that shortest path bridging is one of the most significant enhancements in Ethernet's history.

Ethernet has replaced InfiniBand as the most popular system interconnect of TOP500 supercomputers.

Ethernet has replaced the ATM circuit-switched technology first developed in the early 1990s.

Since 2005, Ethernet enhancements for fiber-optic transmission, longer distances and much higher data rates (e.g. 40 Gbit/s, 100 Gbit/s) are also beginning to adversely impact sales and new deployments of SONET technology

## Varieties of Ethernet

The Ethernet physical layer evolved over a considerable time span and encompasses coaxial, twisted pair and fiber-optic physical media interfaces, with speeds from 10 Mbit/s to 100 Gbit/s, with 400 Gbit/s expected by late 2017. The first introduction of twisted-pair CSMA/CD was StarLAN, standardized as 802.3 1BASE5; while 1BASE5 had little market penetration, it defined the physical apparatus (wire, plug/jack, pin-out, and wiring plan) that would be carried over to 10BASE-T.

The most common forms used are 10BASE-T, 100BASE-TX, and 1000BASE-T. All three utilize twisted pair cables and 8P8C modular connectors. They run at 10 Mbit/s, 100 Mbit/s, and 1 Gbit/s, respectively. Fiber optic variants of Ethernet offer high performance, better electrical isolation and longer distance (tens of kilometers with some versions). In general, network protocol stack software will work similarly on all varieties.

## Frame Structure




A close-up of the SMSC LAN91C110 (SMSC 91x) chip, an embedded Ethernet chip.

In IEEE 802.3, a datagram is called a *packet* or *frame*. *Packet* is used to describe the overall transmission unit and includes the preamble, start frame delimiter (SFD) and

carrier extension (if present).[j] The *frame* begins after the start frame delimiter with a frame header featuring source and destination MAC addresses and a field giving either the protocol type for the payload protocol or the length of the payload. The middle section of the frame consists of payload data including any headers for other protocols (for example, Internet Protocol) carried in the frame. The frame ends with a 32-bit cyclic redundancy check, which is used to detect corruption of data in transit. Notably, Ethernet packets have no time-to-live field, leading to possible problems in the presence of a switching loop.

## AUTONEGOTIATION

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

Autonegotiation is an Ethernet procedure by which two connected devices choose common transmission parameters, such as speed, duplex mode, and flow control. In this process, the connected devices first share their capabilities regarding these parameters and then choose the highest performance transmission mode they both support. In the OSI model, autonegotiation resides in the physical layer. For Ethernet over twisted pair it is defined in clause 28 of IEEE 802.3.

Autonegotiation was originally defined as an optional component in the fast Ethernet standard. It is backwards compatible with the normal link pulses used by 10BASE-T. The protocol was significantly extended in the gigabit Ethernet standard, and is mandatory for 1000BASE-T gigabit Ethernet over twisted pair.

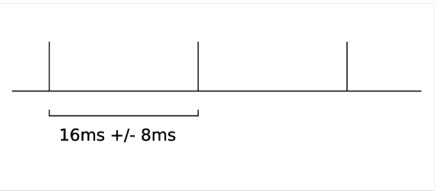
In 1995, a standard was released to allow connected network adapters to negotiate the best possible shared mode of operation. The initial autonegotiation standard contained a mechanism for detecting the speed but not the duplex setting of Ethernet peers that did not use autonegotiation.

Autonegotiation can be used by devices that are capable of different transmission rates, different duplex modes (half duplex and full duplex), and/or different standards at the same speed (though in practice only one standard at each speed is widely supported). Each device declares its *technology abilities*, that is, its possible modes of operation, and the best mode is chosen from those shared by them, with higher speed preferred over lower, and full duplex preferred over half duplex at the same speed.

Parallel detection is used when a device that is capable of autonegotiation is connected to one that is not. This happens if the other device does not support autonegotiation or autonegotiation is administratively disabled. In this condition, the device that is capable of autonegotiation can determine and match speed with the other device. This procedure cannot determine the presence of full duplex, so half duplex is always assumed.

The standards for 1000BASE-T, 1000BASE-TX and 10GBASE-T require autonegotiation to be always present and enabled. Other than speed and duplex mode, autonegotiation is used to communicate the port type (single port or multiport) and the master-slave parameters (whether it is manually configured or not, whether the device is master or slave if this is the case, and the master-slave seed bit otherwise).

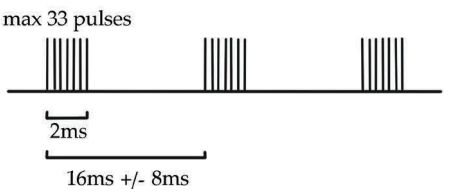
## Electrical Signals




A sequence of normal link pulses, used by 10BASE-T devices to establish link integrity.

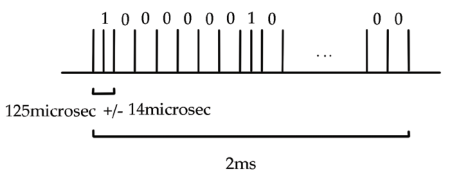
Auto-negotiation (formerly "NWay") is based on pulses similar to those used by 10BASE-T devices to detect the presence of a connection to another device. These *connection present* pulses are sent by Ethernet devices when they are not sending or receiving any frames. They are unipolar positive-only electrical pulses of a nominal duration of 100 ns, with a maximum pulse width of 200 ns, generated at a 16 ms time interval (with a timing variation tolerance of 8 ms). These pulses are called *link integrity test* (LIT) pulses in the 10BASE-T terminology, and are referred to as *normal link pulses* (NLP) in the auto-negotiation specification.

A device detects the failure of a link if neither a frame nor two of the LIT pulses is received for 50-150 ms. For this scheme to work, devices must send LIT pulses regardless of receiving any.




Three bursts of Fast Link Pulses, used by autonegotiating devices to declare their capabilities.

Auto-negotiation uses similar pulses labeled as NLP. NLP are still unipolar, positive-only, and of the nominal duration of 100 ns; but each LIT is replaced by a pulse burst consisting of 17 to 33 pulses sent 125 µs apart. Each such pulse burst is called a **fast link pulse** (FLP) burst. The time interval between the start of each FLP burst is the same 16 milliseconds as between normal link pulses (variation tolerance of 8 ms).




How a link code word (a 16 bit word) is encoded in a fast link pulse burst

The FLP burst consists of 17 NLP at a 125 μs time interval (with a tolerance of 14 μs). Between each pair of two consecutive NLP (i.e. at 62.5 μs after first NLP of the pulse pair) an additional positive pulse may be present. The presence of this additional pulse indicates a logical 1, its absence a logical 0. As a result, every FLP contains a data word of 16 bits. This data word is called a **link code word** (LCW). The bits of the link code word are numbered from 0 to 15, where bit 0 corresponds to the first possible pulse in time and bit 15 to the last.

## The Base Link Code Word

Every fast link pulse burst transmits a word of 16 bits known as a link code word. The first such word is known as a *base link code word*, and its bits are used as follows:

- 0–4: selector field: it indicates which standard is used between IEEE 802.3 and IEEE 802.9;
- 5–12: technology ability field: this is a sequence of bits that encode the possible modes of operations among the 100BASE-T and 10BASE-T modes;
- 13: remote fault: this is set to one when the device is detecting a link failure;
- 14: acknowledgement: the device sets this to one to indicate the correct reception of the base link code word from the other party; this is detected by the reception of at least three identical base code words;
- 15: next page: this bit is used to indicate the intention of sending other link code words after the base link code word;

The technology ability field is composed of eight bits. For IEEE 802.3, these are as follows:

- bit 0: device supports 10BASE-T
- bit 1: device supports 10BASE-T in full duplex
- bit 2: device supports 100BASE-TX
- bit 3: device supports 100BASE-TX in full duplex
- bit 4: device supports 100BASE-T4
- bit 5: pause
- bit 6: asymmetric pause for full duplex
- bit 7: reserved

The acknowledgement bit is used to signal the correct reception of the base code word. This corresponds to having received three identical copies of the base code word. Upon receiving these three identical copies, the device sends a link code word with the acknowledge bit set to one from six times to eight times.

The link code words are also called *pages*. The base link code word is therefore called a base page. The next page bit of the base page is 1 when the device intends to send other pages, which can be used to communicate other abilities. These additional pages are sent only if both devices have sent base pages with a next page bit set to 1.

The additional pages are still encoded as link code words (using 17 clock pulses and up to 16 bit pulses).

## Message and Unformatted Next Page

The base page (the base link code word) is sufficient for devices to advertise which ones among the 10BASE-T, 100BASE-TX and 100BASE-T4 modes they support. For gigabit Ethernet, two other pages are required. These pages are sent if both devices have sent base pages with a next page bit set to one.

The additional pages are of two kinds: *message pages* and *unformatted pages*. These pages are still 16-bit words encoded as pulses in the same way as the base page. Their first eleven bits are data, while their second-to-last bit indicates whether the page is a message page or an unformatted page. The last bit of each page indicates the presence of an additional page.

The 1000BASE-T supported modes and master-slave data (which is used to decide which of the two devices acts as the master, and which one acts as the slave) are sent using a single message page, followed by a single unformatted page. The message page contains:

- half duplex capability
- whether the device is single port or multiport
- whether master/slave is manually configured or not
- whether the device is manually configured as master or slave

The unformatted page contains a 10-bit word, called a master-slave seed value.

## Priority

Upon receipt of the technology abilities of the other device, both devices decide the best possible mode of operation supported by both devices. The priority among modes specified in the 2015 edition of 802.3 is as follows:

- 10GBASE-T full duplex
- 1000BASE-T full duplex
- 1000BASE-T half duplex
- 100BASE-T2 full duplex
- 100BASE-TX full duplex
- 100BASE-T2 half duplex
- 100BASE-T4 half duplex
- 100BASE-TX half duplex
- 10BASE-T full duplex
- 10BASE-T half duplex

In other words, among the modes that are supported by both devices, each device chooses the one that is the topmost in this list.

## Interoperability Problems

The first version of the autonegotiation specification, IEEE 802.3u, was open to different interpretations. Although most manufacturers implemented this standard in one way, some others, including network giant Cisco, implemented it in a different way. Autonegotiation between devices that implemented it differently failed. Problems like this with autonegotiation led many network administrators to manually set the speed and duplex mode of each network interface card. However, the use of manually set configuration may also lead to duplex mismatches, in particular when two connected devices are:

- One manually set to half duplex and one manually set to full duplex
- One set to autonegotiation and one manually set to full duplex

Duplex mismatch problems are difficult to diagnose because the network is apparently working, and simple programs used for network tests such as ping report a valid connection; however, the network is much slower than expected.

The debatable portions of the autonegotiation specifications were eliminated by the 1998 release of 802.3. This was later followed by the release of IEEE 802.3ab in 1999. The new standard specified that gigabit Ethernet over copper wiring requires autonegotiation. Currently, most network equipment manufacturers recommend using autonegotiation on all access ports and enable it as a factory default setting.

## Duplex Mismatch

A duplex mismatch occurs when two connected devices are configured in different duplex modes. This may happen for example if one is configured for autonegotiation while the other one has a fixed mode of operation that is full duplex (no autonegotiation). In such conditions, the autonegotiation device correctly detects the speed of operation, but is unable to correctly detect the duplex mode. As a result, it sets the correct speed but starts using the half duplex mode.

When a device is operating in full duplex while the other one operates in half duplex, the connection works at a very low speed if both devices attempt to send frames at the same time. This is because data can be sent in both directions at the same time in full duplex mode, but only in one direction at a time in half duplex mode. As a result, a full duplex device may transmit data while it is receiving. However, if the other device is working in half duplex, it does not expect to receive data (because it is currently sending); therefore, it senses a collision and attempts to resend the frame it was sending. Depending on timing the half duplex device may sense a late collision, which it will interpret as a hard error rather than a normal consequence of CSMA/CD and will not attempt to resend the frame. On the other hand, the full duplex device does not detect any collision and does not resend the frame, even if the other device has discarded it as corrupted by collision. Still, the full duplex device, not expecting incoming frames to be truncated by collision detection, will report frame check sequence errors. This

combination of **late** collisions reported at the half-duplex end and FCS errors reported by the full duplex end can be used as an indication that a duplex mismatch is present.

This packet loss happens when both devices are transmitting at the same time. This may happen even when the link is used, from the user's perspective, in one direction only. A TCP stream requires all packets sent to be acknowledged by the receiving device. As a result, even if actual data is sent in one direction only, collision may be generated with acknowledgement packets traveling in the other direction.

The protocol that became IEEE 802.3 clause 28 was developed from a patented technology by National Semiconductor known as NWay. The company gave a letter of assurance for anyone to use their system for a one time license fee. Another company has since bought the rights to that patent.

## Patents

Autonegotiation is covered by the US patents U.S. Patent 5,617,418; U.S. Patent 5,687,174; E U.S. Patent RE39,405 E; E U.S. Patent RE39,116 E; 971,018 (filed 1992-11-02); 146,729 (filed 1993-11-01); 430,143 (filed 1995-04-26)

European Patent Applications SN 93308568.0 (DE, FR, GB, IT, NL); Korean Patent No. 286791, Taiwanese Patent No. 098359, Japanese Patent No. 3705610; Japanese Patent 4234. Applications SN H5-274147; Korean Patent Applications SN 22995/93; Taiwanese Patent Applications SN 83104531;

# REFERENCES


1. Ralph Santitoro (2003). "Metro Ethernet Services – A Technical Overview" (PDF). mef.net. Retrieved 2016-01-09.
2. "IEEE 802.3 'Standard for Ethernet' Marks 30 Years of Innovation and Global Market Growth" (Press release). IEEE. June 24, 2013. Retrieved January 11, 2014.
3. Xerox (August 1976). "Alto: A Personal Computer System Hardware Manual" (PDF). Xerox. p. 37. Retrieved 25 August 2015.
4. Charles M. Kozierok (2005-09-20). "Data Link Layer (Layer 2)". tcpipguide.com. Retrieved 2016-01-09.
5. Joe Jensen (2007-10-26). "802.11 g: Pros & Cons of a Wireless Network in a Business Environment". networkbits.net. Retrieved 2016-01-09.
6. The History of Ethernet. NetEvents.tv. 2006. Retrieved September 10, 2011.
7. "Ethernet Prototype Circuit Board". Smithsonian National Museum of American History. 1973. Retrieved September 2, 2007.
8. Gerald W. Brock (September 25, 2003). The Second Information Revolution. Harvard University Press. p. 151. ISBN 0-674-01178-3.
9. Cade Metz (March 13, 2009). "Ethernet — a networking protocolname for the ages: Michelson, Morley, and Metcalfe". The Register: 2. Retrieved March 4, 2013.

10. Mary Bellis. “Inventors of the Modern Computer”. About.com. Retrieved September 10, 2011.
11. U.S. Patent 4,063,220 “Multipoint data communication system (with collision detection)”
12. Robert Metcalfe; David Boggs (July 1976). “Ethernet: Distributed Packet Switching for Local Computer Networks” (PDF). Communications of the ACM. 19 (7): 395–405. doi:10.1145/360248.360253.
13. John F. Shoch; Yogen K. Dalal; David D. Redell; Ronald C. Crane (August 1982). “Evolution of the Ethernet Local Computer Network”(PDF). IEEE Computer. 15 (8): 14–26. doi:10.1109/MC.1982.1654107.
14. von Burg, Urs; Kenney, Martin (December 2003). “Sponsors, Communities, and Standards: Ethernet vs. Token Ring in the Local Area Networking Business” (PDF). Industry & Innovation. 10 (4): 351–375. doi:10.1080/136627103200016 3621. Archived from the original on 2012-03-21. Retrieved 17 February 2014.
15. Digital Equipment Corporation; Intel Corporation; Xerox Corporation (30 September 1980). “The Ethernet, A Local Area Network. Data Link Layer and Physical Layer Specifications, Version 1.0” (PDF). Xerox Corporation. Retrieved 2011-12-10.
16. Digital Equipment Corporation; Intel Corporation; Xerox Corporation (November 1982). “The Ethernet, A Local Area Network. Data Link Layer and Physical Layer Specifications, Version 2.0” (PDF). Xerox Corporation. Retrieved 2011-12-10.
17. Robert Breyer; Sean Riley (1999). Switched, Fast, and Gigabit Ethernet. Macmillan. ISBN 1-57870-073-6.
18. Jamie Parker Pearson (1992). Digital at Work. Digital Press. p. 163. ISBN 1-55558-092-0.
19. Rick Merritt (December 20, 2010). “Shifts, growth ahead for 10G Ethernet”. E Times. Retrieved September 10, 2011.
20. “My oh My – Ethernet Growth Continues to Soar; Surpasses Legacy”. Telecom News Now. July 29, 2011. Retrieved September 10, 2011.
21. Jim Duffy (February 22, 2010). “Cisco, Juniper, HP drive Ethernet switch market in Q4”. Network World. Retrieved September 10, 2011.
22. Vic Hayes (August 27, 2001). “Letter to FCC” (PDF). Retrieved October 22, 2010. IEEE 802 has the basic charter to develop and maintain networking standards... IEEE 802 was formed in February 1980...
23. IEEE 802.3-2008, p.iv
24. “ISO 8802-3:1989”. ISO. Retrieved 2015-07-08.
25. Jim Duffy (2009-04-20). “Evolution of Ethernet”. Network World. Retrieved 2016-01-01.
26. Douglas E. Comer (2000). Internetworking with TCP/IP – Principles, Protocols and Architecture (4th ed.). Prentice Hall. ISBN 0-13-018380-6.2.4.9 – Ethernet

Hardware Addresses, p. 29, explains the filtering.

27. Iljitsch van Beijnum. "Speed matters: how Ethernet went from 3Mbps to 100Gbps... and beyond". Ars Technica. Retrieved July 15, 2011. All aspects of Ethernet were changed: its MAC procedure, the bit encoding, the wiring... only the packet format has remained the same.
28. Fast Ethernet Turtorial, Lantronix, retrieved 2016-01-01
29. Geetaj Channana (November 1, 2004). "Motherboard Chipsets Roundup". PCQuest. Retrieved October 22, 2010. While comparing motherboards in the last issue we found that all motherboards support Ethernet connection on board.
30. Charles E. Spurgeon (2000). Ethernet: The Definitive Guide. O'Reilly. ISBN 978-1-56592-660-8.
31. Heinz-Gerd Hegering; Alfred Lapple (1993). Ethernet: Building a Communications Infrastructure. Addison-Wesley. ISBN 0-201-62405-2.
32. Ethernet Tutorial – Part I: Networking Basics, Lantronix, retrieved 2016-01-01
33. Shoch, John F.; Hupp, Jon A. (December 1980). "Measured performance of an Ethernet local network". Communications of the ACM. ACM Press. 23 (12): 711–721. doi:10.1145/359038.359044. ISSN 0001-0782.
34. Boggs, D.R.; Mogul, J.C. & Kent, C.A. (September 1988). "Measured capacity of an Ethernet: myths and reality" (PDF). DEC WRL.
35. Eric G. Rawson; Robert M. Metcalfe (July 1978). "Fibemet: Multimode Optical Fibers for Local Computer Networks" (PDF). IEEE Transactions on Communications. 26 (7): 983–990. doi:10.1109/TCOM.1978.1094189. Retrieved June 11, 2011.
36. Spurgeon, Charles E. (2000). Ethernet; The Definitive Guide. Nutshell Handbook. O'Reilly. p. 29. ISBN 1-56592-660-9.
37. Urs von Burg (2001). The Triumph of Ethernet: technological communities and the battle for the LAN standard. Stanford University Press. p. 175. ISBN 0-8047-4094-1.
38. "Token Ring-to-Ethernet Migration". Cisco. Retrieved October 22, 2010. Respondents were first asked about their current and planned desktop LAN attachment standards. The results were clear—switched Fast Ethernet is the dominant choice for desktop connectivity to the network
39. Allan, David; Bragg, Nigel (2012). 802.1aq Shortest Path Bridging Design and Evolution : The Architects' Perspective. New York: Wiley. ISBN 978-1-118-14866-2.
40. "HIGHLIGHTS - JUNE 2016". June 2016. Retrieved 2016-08-08. InfiniBand technology is now found on 205 systems, down from 235 systems, and is now the second most-used internal system interconnect technology. Gigabit Ethernet has risen to 218 systems up from 182 systems, in large part thanks to 176 systems now using 10G interfaces.

41. "Adopted Timeline" (PDF). IEEE 802.3bs Task Force. 2014-05-19. Retrieved 2015-02-24.
42. "1BASE5 Medium Specification (StarLAN)". cs.nthu.edu.tw. 1996-12-28. Retrieved 2014-11-11.
43. "802.3-2012 - IEEE Standard for Ethernet" (PDF). ieee.org. IEEE Standards Association. 2012-12-28. Retrieved 2014-02-08.
44. "Clause 28: Physical Layer link signaling for Auto-Negotiation on twisted pair", IEEE 802.3 (PDF), p. 221, (registration required (help))
45. Jayaswal, Kailash (2005). Administering Data Centers Servers, Storage, and Voice over IP. Hoboken: John Wiley & Sons. p. 168. ISBN 0471783358.
46. Schmidt, Daniel Minoli, Andrew (1998). Switched network services. New York: Wiley Computer Pub. p. 93. ISBN 0471190802.
47. IEEE. "Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and Physical Layer specifications" (PDF). SECTION TWO: This section includes Clause21 through Clause 33 and Annex 22A through Annex 33E. Retrieved 2014-06-03.
48. "IEEE Link Task Force Autodetect, Specification for NWay Autodetect" (PDF). p. 57. Archived from the original (PDF) on 2011-07-14.
49. IEEE 802.3 Annex 28B
50. "Configuring and Troubleshooting Ethernet 10/100/1000Mb Half/Full Duplex Auto-Negotiation". Cisco. Retrieved 2012-01-12. Cisco recommends to leave auto-negotiation on for those devices compliant with 802.3u.
51. Jim Eggers and Steve Hodnett (July 2004). "Ethernet Autonegotiation Best Practices" (PDF). Sun Microsystems. Archived from the original (PDF)on 2011-05-20. Using autonegotiation is the IEEE 802.3 standard and customers are encouraged to follow the "intent" of IEEE 802.3u/z standards and implement autonegotiation in their Ethernet environments.
52. Rich Hernandez (2001). "Gigabit Ethernet Auto-Negotiation". Dell. Retrieved 2012-01-12.
53. "Archived copy" (PDF). Archived from the original (PDF) on 2008-11-19. Retrieved 2009-12-02.
54. Negotiated Data Solutions LLC. "NWay/IEEE Standard Patent License Offer | Negotiated Data Solutions LLC". Negotiateddata.com. Archived from the original on 2009-01-06. Retrieved 2010-02-02.

CHAPTER 7

# ARPANET

## Chapter Contents


- **Introduction**
- **Bitnet**
- **Cellular Network**
- **Cyclades**

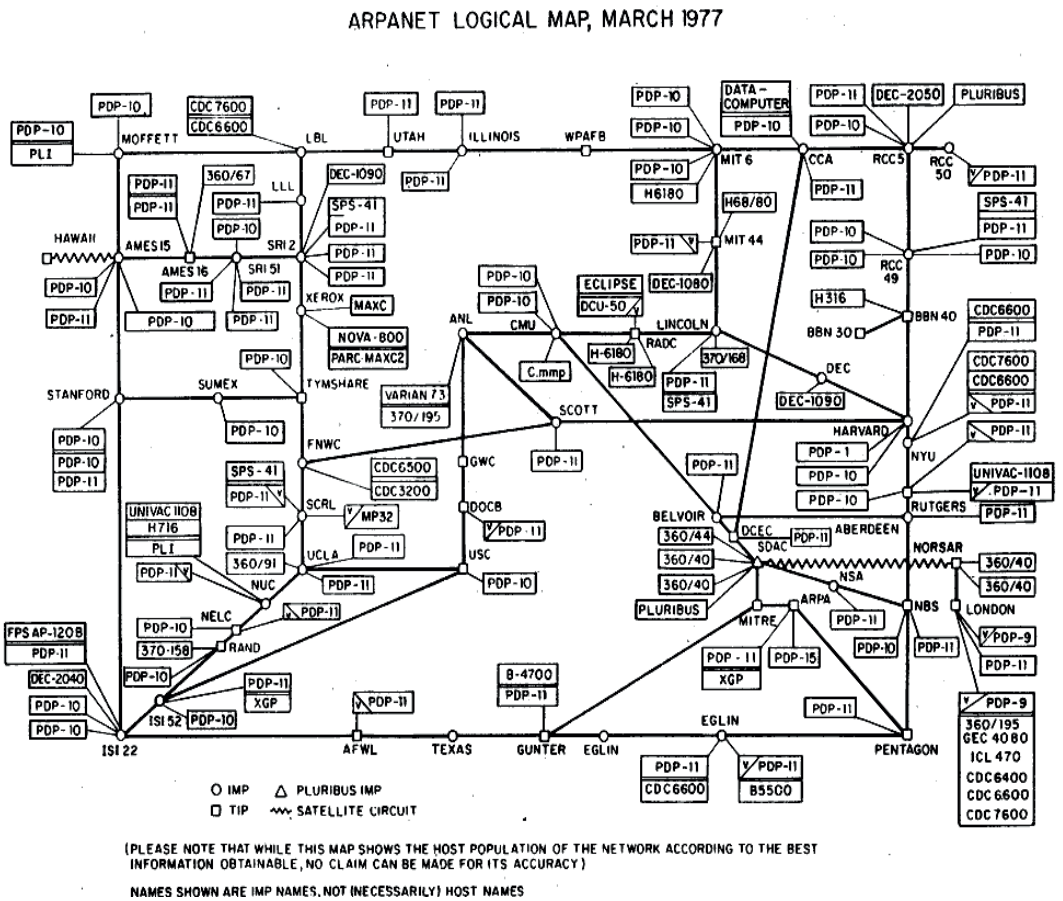

The Advanced Research Projects Agency Network (ARPANET) was one of the main precursors to the Internet. At the time it was conceived, most communications were thought of in terms of circuit switching, but ARPANET implemented the type of packet switching network that would come to dominate communications around the world. The network was based on the principle of creating small data packets that could be sent across the network link at any time it was available, rather than securing a circuit, like would be required in a circuit switching network.

## INTRODUCTION

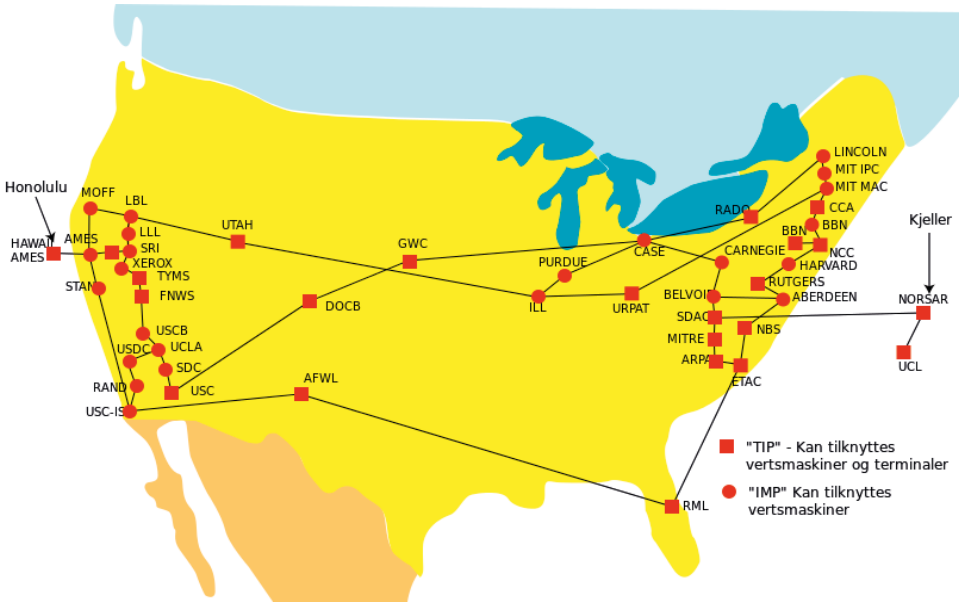
The Advanced Research Projects Agency Network (ARPANET) was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet. ARPANET was initially funded by the Advanced Research Projects Agency (ARPA) of the United States Department of Defense.

The packet switching methodology employed in the ARPANET was based on concepts and designs by Americans Leonard Kleinrock and Paul Baran, British scientist Donald Davies, and Lawrence Roberts. The TCP/IP communications protocols were developed for ARPANET by computer scientists Robert Kahn and Vint Cerf, and incorporated concepts from the French CYCLADES project directed by Louis Pouzin.

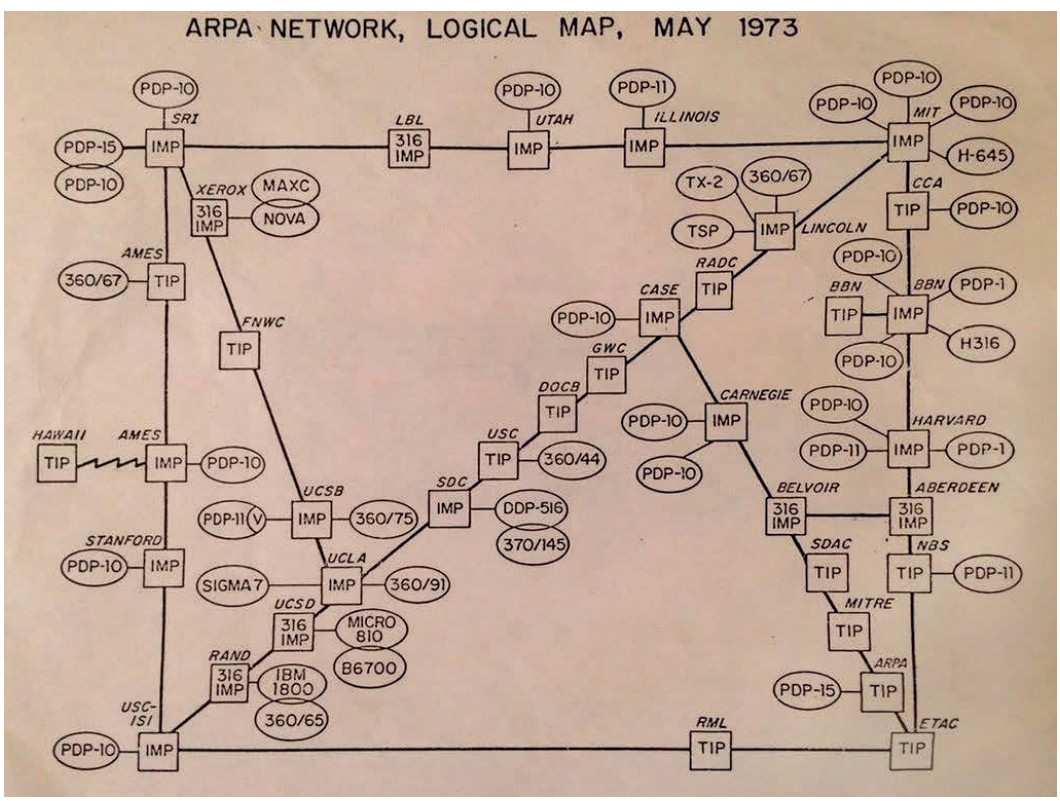
As the project progressed, protocols for internetworking were developed by which multiple separate networks could be joined into a network of networks. Access to the ARPANET was expanded in 1981 when the National Science Foundation (NSF) funded the Computer Science Network (CSNET). In 1982, the Internet protocol suite (TCP/IP) was introduced as the standard networking protocol on the ARPANET. In the early 1980s the NSF funded the establishment for national supercomputing centers at several universities, and provided interconnectivity in 1986 with the NSFNET project, which also created network access to the supercomputer sites in the United States from research and education organizations. ARPANET was decommissioned in 1990.




ARPANET logical map, March 1977




Arpanet 1974




Arpanet 1973

Packet switching—today the dominant basis for data communications worldwide—was a new concept at the time of the conception of the ARPANET. Prior to the advent of packet switching, both voice and data communications had been based on the idea of circuit switching, as in the traditional telephone circuit, wherein each telephone call is allocated a dedicated, end to end, electronic connection between the two communicating stations. Such stations might be telephones or computers. The (temporarily) dedicated line typically comprises many intermediary lines which are assembled into a chain that stretches all the way from the originating station to the destination station. With packet switching, a data system could use a single communication link to communicate with more than one machine by collecting data into datagrams and transmitting these as packets onto the attached network link, as soon as the link becomes idle. Thus, not only can the link be shared, much as a single post box can be used to post letters to different destinations, but each packet can be routed independent of other packets.

The earliest ideas for a computer network intended to allow general communications among computer users were formulated by computer scientist J. C. R. Licklider of Bolt, Beranek and Newman (BBN), in April 1963, in memoranda discussing the concept of the "Intergalactic Computer Network". Those ideas encompassed many of the features of the contemporary Internet. In October 1963, Licklider was appointed head of the Behavioral Sciences and Command and Control programs at the Defense Department's Advanced Research Projects Agency (ARPA). He convinced Ivan Sutherland and Bob Taylor that this network concept was very important and merited development, although Licklider left ARPA before any contracts were assigned for development.

Sutherland and Taylor continued their interest in creating the network, in part, to allow ARPA-sponsored researchers at various corporate and academic locales to utilize computers provided by ARPA, and, in part, to quickly distribute new software and other computer science results.Taylor had three computer terminals in his office, each connected to separate computers, which ARPA was funding: one for the System Development Corporation (SDC) Q-32 in Santa Monica, one for Project Genie at the University of California, Berkeley, and another for Multics at the Massachusetts Institute of Technology. Taylor recalls the circumstance: "For each of these three terminals, I had three different sets of user commands. So, if I was talking online with someone at S.D.C., and I wanted to talk to someone I knew at Berkeley, or M.I.T., about this, I had to get up from the S.D.C. terminal, go over and log into the other terminal and get in touch with them. I said, "Oh Man!», it's obvious what to do: If you have these three terminals, there ought to be one terminal that goes anywhere you want to go. That idea is the ARPANET".

Meanwhile, since the early 1960s, Paul Baran at the RAND Corporation had been researching systems that could survive nuclear war and developed the idea of *distributed adaptive message block switching*. Donald Davies at the United Kingdom's National Physical Laboratory (NPL) independently invented the same concept in 1965. His work, presented by a colleague, initially caught the attention of ARPANET developers at a conference in Gatlinburg, Tennessee, in October 1967. He gave the first public demonstration, having coined the term *packet switching*, on 5 August 1968 and incorporated it into the NPL network in England. Larry Roberts at ARPA applied Davies' concepts of packet switching for the ARPANET. The NPL network followed by ARPANET were the first two networks in the world to use packet switching, and were themselves connected together in 1973.

The NPL network was using line speeds of 768 kbit/s, and the proposed line speed for ARPANET was upgraded from 2.4 kbit/s to 50 kbit/s.

## Creation

By mid-1968, Taylor had prepared a complete plan for a computer network, and, after ARPA's approval, a Request for Quotation (RFQ) was issued for 140 potential bidders. Most computer science companies regarded the ARPA–Taylor proposal as outlandish, and only twelve submitted bids to build a network; of the twelve, ARPA regarded only four as top-rank contractors. At year's end, ARPA considered only two contractors, and awarded the contract to build the network to BBN Technologies on 7 April 1969. The initial, seven-person BBN team were much aided by the technical specificity of their response to the ARPA RFQ, and thus quickly produced the first working system. This team was led by Frank Heart. The BBN-proposed network closely followed Taylor's ARPA plan: a network composed of small computers called Interface Message Processors (or IMPs), similar to the later concept of routers, that functioned as gateways interconnecting local resources. At each site, the IMPs performed store-and-forward packet switching functions, and were interconnected with leased lines via telecommunication data sets (modems), with initial data rates of 56kbit/s. The host computers were connected to the IMPs via custom serial communication interfaces. The system, including the hardware and the packet switching software, was designed and installed in nine months.

The first-generation IMPs were built by BBN Technologies using a rugged computer version of the Honeywell DDP-516 computer configured with 24KB of expandable magnetic-core memory, and a 16-channel Direct Multiplex Control (DMC) direct memory access unit. The DMC established custom interfaces with each of the host computers and modems. In addition to the front-panel lamps, the DDP-516 computer also features a special set of 24 indicator lamps showing the status of the IMP communication channels. Each IMP could support up to four local hosts, and could communicate with up to six remote IMPs via leased lines. The network connected one computer in Utah with three in California. Later, the Department of Defense allowed the universities to join the network for sharing hardware and software resources.

## Debate on Design Goals

In *A Brief History of the Internet*, the Internet Society denies that ARPANET was designed to survive a nuclear attack:

It was from the RAND study that the false rumor started, claiming that the ARPANET was somehow related to building a network resistant to nuclear war. This was never true of the ARPANET; only the unrelated RAND study on secure voice considered nuclear war. However, the later work on Internetting did emphasize robustness and survivability, including the capability to withstand losses of large portions of the underlying networks.

The RAND study was conducted by Paul Baran and pioneered packet switching. In an interview he confirmed that while ARPANET did not exactly share his project's goal, his work had greatly contributed to the development of ARPANET. Minutes taken by Elmer Shapiro of Stanford Research Institute at the ARPANET design meeting of 9–10

Oct. 1967 indicate that a version of Baran's routing method and suggestion of using a fixed packet size was expected to be employed.

According to Stephen J. Lukasik, who as Deputy Director and Director of DARPA (1967–1974) was "the person who signed most of the checks for Arpanet's development":

The goal was to exploit new computer technologies to meet the needs of military command and control against nuclear threats, achieve survivable control of US nuclear forces, and improve military tactical and management decision making.

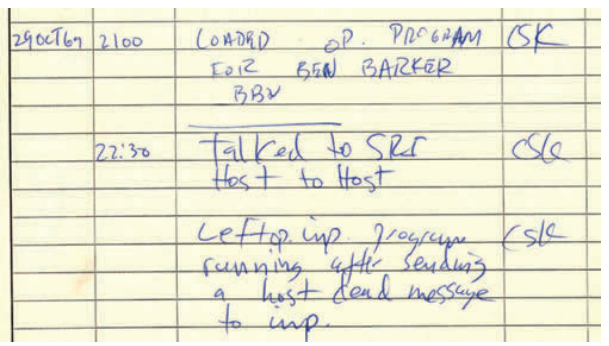
The ARPANET incorporated distributed computation (and frequent re-computation) of routing tables. This was a major contribution to the survivability of the ARPANET in the face of significant destruction - even by a nuclear attack. Such auto-routing was technically quite challenging to construct at the time. The fact that it was incorporated into the early ARPANET made many believe that this had been a design goal.

The ARPANET was designed to survive subordinate-network losses, since the principal reason was that the switching nodes and network links were unreliable, even without any nuclear attacks. Resource scarcity supported the creation of the ARPANET, according to Charles Herzfeld, ARPA Director (1965–1967):

The ARPANET was not started to create a Command and Control System that would survive a nuclear attack, as many now claim. To build such a system was, clearly, a major military need, but it was not ARPA's mission to do this; in fact, we would have been severely criticized had we tried. Rather, the ARPANET came out of our frustration that there were only a limited number of large, powerful research computers in the country, and that many research investigators, who should have access to them, were geographically separated from them.

The ARPANET was operated by the military during the two decades of its existence, until 1990.

## Deployment




**Historical document:** First ARPANET IMP log: the first message ever sent via the ARPANET, 10:30 pm, 29 October 1969. This IMP Log excerpt, kept at UCLA, describes setting up a message transmission from the UCLA SDS Sigma 7 Host computer to the SRI SDS 940 Host computer.

The initial ARPANET consisted of four IMPs:

- University of California, Los Angeles (UCLA), where Leonard Kleinrock had established a Network Measurement Center, with an SDS Sigma 7 being the first computer attached to it;
- The Augmentation Research Center at Stanford Research Institute (now SRI International), where Douglas Engelbart had created the ground-breaking NLS system, a very important early hypertext system, and would run the Network Information Center (NIC), with the SDS 940 that ran NLS, named "Genie", being the first host attached;
- University of California, Santa Barbara (UCSB), with the Culler-Fried Interactive Mathematics Center's IBM 360/75, running OS/MVT being the machine attached;
- The University of Utah's Computer Science Department, where Ivan Sutherland had moved, running a DEC PDP-10 operating on TENEX.

The first successful message on the ARPANET was sent by UCLA student programmer Charley Kline, at 10:30 pm on 29 October 1969, from Boelter Hall 3420. Kline transmitted from the university's SDS Sigma 7 Host computer to the Stanford Research Institute's SDS 940 Host computer. The message text was the word *login*; on an earlier attempt the *l* and the *o* letters were transmitted, but the system then crashed. Hence, the literal first message over the ARPANET was *lo*. About an hour later, after the programmers repaired the code that caused the crash, the SDS Sigma 7 computer effected a full *login*. The first permanent ARPANET link was established on 21 November 1969, between the IMP at UCLA and the IMP at the Stanford Research Institute. By 5 December 1969, the entire four-node network was established.

## Growth and Evolution

In March 1970, the ARPANET reached the East Coast of the United States, when an IMP at BBN in Cambridge, Massachusetts was connected to the network. Thereafter, the ARPANET grew: 9 IMPs by June 1970 and 13 IMPs by December 1970, then 18 by September 1971 (when the network included 23 university and government hosts); 29 IMPs by August 1972, and 40 by September 1973. By June 1974, there were 46 IMPs, and in July 1975, the network numbered 57 IMPs. By 1981, the number was 213 host computers, with another host connecting approximately every twenty days.

In 1973 a transatlantic satellite link connected the Norwegian Seismic Array (NORSAR) to the ARPANET, making Norway the first country outside the US to be connected to the network. At about the same time a terrestrial circuit added a London IMP.

In 1975, the ARPANET was declared "operational". The Defense Communications Agency took control since ARPA was intended to fund advanced research.

In September 1984 work was completed on restructuring the ARPANET giving U.S. military sites their own Military Network (MILNET) for unclassified defense department communications. Controlled gateways connected the two networks. The combination was called the Defense Data Network (DDN). Separating the civil and military networks reduced the 113-node ARPANET by 68 nodes. The MILNET later became the NIPRNet.

## Rules and Etiquette

Because of its government funding, certain forms of traffic were discouraged or prohibited. A 1982 handbook on computing at MIT's AI Lab stated regarding network etiquette:

It is considered illegal to use the ARPANet for anything which is not in direct support of Government business ... personal messages to other ARPANet subscribers (for example, to arrange a get-together or check and say a friendly hello) are generally not considered harmful ... Sending electronic mail over the ARPANet for commercial profit or political purposes is both anti-social and illegal. By sending such messages, you can offend many people, and it is possible to get MIT in serious trouble with the Government agencies which manage the ARPANet.

## Technology

Support for inter-IMP circuits of up to 230.4 kbit/s was added in 1970, although considerations of cost and IMP processing power meant this capability was not actively used.

1971 saw the start of the use of the non-ruggedized (and therefore significantly lighter) Honeywell 316 as an IMP. It could also be configured as a Terminal Interface Processor (TIP), which provided terminal server support for up to 63 ASCII serial terminals through a multi-line controller in place of one of the hosts. The 316 featured a greater degree of integration than the 516, which made it less expensive and easier to maintain. The 316 was configured with 40 kB of core memory for a TIP. The size of core memory was later increased, to 32 kB for the IMPs, and 56 kB for TIPs, in 1973.

In 1975, BBN introduced IMP software running on the Pluribus multi-processor. These appeared in a few sites. In 1981, BBN introduced IMP software running on its own C/30 processor product.

In 1983, TCP/IP protocols replaced NCP as the ARPANET's principal protocol, and the ARPANET then became one subnet of the early Internet.

The original IMPs and TIPs were phased out as the ARPANET was shut down after the introduction of the NSFNet, but some IMPs remained in service as late as July 1990.

The *ARPANET Completion Report*, jointly published by BBN and ARPA, concludes that:

... it is somewhat fitting to end on the note that the ARPANET program has had a strong and direct feedback into the support and strength of computer science, from which the network, itself, sprang.

In the wake of ARPANET being formally decommissioned on 28 February 1990, Vinton Cerf wrote the following lamentation, entitled "Requiem of the ARPANET":

It was the first, and being first, was best,but now we lay it down to ever rest.Now pause with me a moment, shed some tears.For auld lang syne, for love, for years and yearsof faithful service, duty done, I weep.Lay down thy packet, now, O friend, and sleep.

-Vinton Cerf

Senator Albert Gore, Jr. authored the High Performance Computing and Communication Act of 1991, commonly referred to as "The Gore Bill", after hearing the 1988 concept for a National Research Network submitted to Congress by a group chaired by Leonard Kleinrock. The bill was passed on 9 December 1991 and led to the National Information Infrastructure (NII) which Al Gore called the *information superhighway*.

The ARPANET project was honored with two IEEE Milestones, both dedicated in 2009.

## Software and Protocols

The starting point for host-to-host communication on the ARPANET in 1969 was the 1822 protocol, which defined the transmission of messages to an IMP. The message format was designed to work unambiguously with a broad range of computer architectures. An 1822 message essentially consisted of a message type, a numeric host address, and a data field. To send a data message to another host, the transmitting host formatted a data message containing the destination host's address and the data message being sent, and then transmitted the message through the 1822 hardware interface. The IMP then delivered the message to its destination address, either by delivering it to a locally connected host, or by delivering it to another IMP. When the message was ultimately delivered to the destination host, the receiving IMP would transmit a *Ready for Next Message* (RFNM) acknowledgement to the sending, host IMP.

Unlike modern Internet datagrams, the ARPANET was designed to reliably transmit 1822 messages, and to inform the host computer when it loses a message; the contemporary IP is unreliable, whereas the TCP is reliable. Nonetheless, the 1822 protocol proved inadequate for handling multiple connections among different applications residing in a host computer. This problem was addressed with the Network Control Program (NCP), which provided a standard method to establish reliable, flow-controlled, bidirectional communications links among different processes in different host computers. The NCP interface allowed application software to connect across the ARPANET by implementing higher-level communication protocols, an early example of the *protocol layering* concept incorporated to the OSI model.

In 1983, TCP/IP protocols replaced NCP as the ARPANET's principal protocol, and the ARPANET then became one component of the early Internet.

### *Network Applications*

NCP provided a standard set of network services that could be shared by several applications running on a single host computer. This led to the evolution of *application protocols* that operated, more or less, independently of the underlying network service, and permitted independent advances in the underlying protocols.

In 1971, Ray Tomlinson, of BBN sent the first network e-mail (RFC 524, RFC 561). By 1973, e-mail constituted 75 percent of ARPANET traffic.

By 1973, the File Transfer Protocol (FTP) specification had been defined (RFC 354) and implemented, enabling file transfers over the ARPANET.

The Network Voice Protocol (NVP) specifications were defined in 1977 (RFC 741), then implemented, but, because of technical shortcomings, conference calls over the ARPANET never worked well; the contemporary Voice over Internet Protocol (packet voice) was decades away.

### *Password Protection*

The Purdy Polynomial hash algorithm was developed for ARPANET to protect passwords in 1971 at the request of Larry Roberts, head of ARPA at that time. It computed a polynomial of degree $2^{24} + 17$ modulo the 64-bit prime $p = 2^{64} - 59$. The algorithm was later used by Digital Equipment Corporation (DEC) to hash passwords in the VMS Operating System, and is still being used for this purpose.

## Arpanet in Popular Culture

1. *Computer Networks: The Heralds of Resource Sharing*, a 30-minute documentary film featuring Fernando J. Corbato, J.C.R. Licklider, Lawrence G. Roberts, Robert Kahn, Frank Heart, William R. Sutherland, Richard W. Watson, John R. Pasta, Donald W. Davies, and economist, George W. Mitchell.
2. "Scenario", a February 1985 episode of the U.S. television sitcom *Benson* (season 6, episode 20), was the first incidence of a popular TV show directly referencing the Internet or its progenitors. The show includes a scene in which the ARPANET is accessed.
3. There is an electronic music artist known as "Arpanet", Gerald Donald, one of the members of Drexciya. The artist's 2002 album *Wireless Internet* features commentary on the expansion of the internet via wireless communication, with songs such as *NTT DoCoMo*, dedicated to the mobile communications giant based in Japan.
4. Thomas Pynchon mentions ARPANET in his 2009 novel *Inherent Vice*, which is set in Los Angeles in 1970, and in his 2013 novel *Bleeding Edge*.
5. The 1993 television series *The X-Files* featured the ARPANET in a season 5 episode, titled "Unusual Suspects". John Fitzgerald Byers offers to help Susan Modeski (known as Holly . . . "just like the sugar") by hacking into the ARPANET to obtain sensitive information.
6. In the spy-drama television series *The Americans*, a Russian scientist defector offers access to ARPANET to the Russians in a plea to not be repatriated (Season 2 Episode 5 "The Deal"). Episode 7 of Season 2 is named 'ARPANET' and features Russian infiltration to bug the network.
7. In the television series *Person of Interest*, main character Harold Finch hacked ARPANET in 1980 using a homemade computer during his first efforts to built a prototype of the Machine. This corresponds with the real life virus that occurred in October of that year that temporarily halted ARPANET functions. The ARPANET hack was first discussed in the episode *2PiR* where a computer science teacher called it the most famous hack in history and one that was

never solved. Finch later mentioned it to Person of Interest Caleb Phipps and his role was first indicated when he showed knowledge that it was done by "a kid with a homemade computer" which Phipps, who had researched the hack, had never heard before.

8. In the third season of the television series *Halt and Catch Fire*, the character Joe MacMillan explores the potential commercialization of ARPANET.

# BITNET

BITNET was a co-operative U.S. university computer network founded in 1981 by Ira Fuchs at the City University of New York (CUNY) and Greydon Freeman, Inc. at Yale University. The first network link was between CUNY and Yale.

The name BITNET originally meant "Because It's There Network", but it eventually came to mean "Because It's Time Network".

A college or university wishing to join BITNET was required to a lease a data circuit (phone line) from a site to an existing BITNET node, buy modems for each end of the data circuit, sending one to the connecting point site, and allow other institutions to connect to its site free of charge.

## Technical Details

Bitnet's NJE (Network Job Entry) network protocols, called RSCS, were used for the huge IBM internal network known as VNET. BITNET links originally ran at 9600 baud. The BITNET protocols were eventually ported to non-IBM mainframe operating systems, and became particularly widely implemented under VAX/VMS, in addition to DECnet.

BITNET featured email and LISTSERV software, but predated the World Wide Web, the common use of FTP, and Gopher. Gateways for the lists made them available on Usenet. BITNET also supported interactive transmission of files and messages to other users. A gateway service called TRICKLE enabled users to request files from Internet FTP servers in 64 Kb UUencoded chunks. The *Interchat Relay Network*, popularly known as Bitnet Relay, was the network's instant messaging feature.

BITNET differed from the Internet in that it was a point-to-point "store and forward" network. That is, email messages and files were transmitted in their entirety from one server to the next until reaching their destination. From this perspective, BITNET was more like UUCPNET.

BITNET's first electronic magazine, VM/COM, began as a University of Maine newsletter and circulated broadly in early 1984. Two email newsletters that began as Bitnet newsletters in the fall of 1987 are known to still be transmitting. They are the Electronic Air and SCUP Email News (formerly SCUP Bitnet News).

BITNET's eligibility requirements limited exchange with commercial entities, including IBM itself, which made technical assistance and bug fixes difficult. This became a particular problem when trying to communicate on heterogeneous networks with graphical workstation vendors such as Silicon Graphics.

## Extent

At its zenith around 1991, BITNET extended to almost 500 organizations and 3,000 nodes, all educational institutions. It spanned North America (in Canada it was known as NetNorth), Europe (as EARN), Israel (as ISRAEARN), India (VIDYANET) and some Persian Gulf states (as GulfNet). BITNET was also very popular in other parts of the world, especially in South America, where about 200 nodes were implemented and heavily used in the late 1980s and early 1990s. With the rapid growth of TCP/IP systems and the Internet in the early 1990s, and the rapid abandonment of the base IBM mainframe platform for academic purposes, BITNET's popularity and use diminished quickly.

## Legacy

In 1984, a text-based BITNET game called MAD became the first global Multi-User Dungeon (MUD). Players connected from the United States, Europe or Israel to a single server running in France.

In 1996, CREN ended their support for BITNET. The individual nodes were free to keep their phone lines up as long as they wished, but as nodes dropped out, the network splintered into parts that were inaccessible from each other. As of 2007, BITNET has essentially ceased operation. However, a successor, BITNET II, which transmits information via the Internet using BITNET protocols, still has some users.

# CELLULAR NETWORK

A **cellular network** or **mobile network** is a communication network where the last link is wireless. The network is distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. This base station provides the cell with the network coverage which can be used for transmission of voice, data and others. A cell might use a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed service quality within each cell.

When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

Cellular networks offer a number of desirable features:

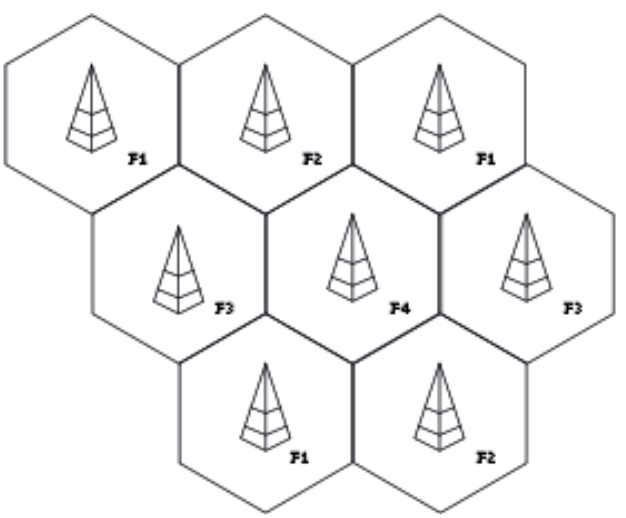
- More capacity than a single large transmitter, since the same frequency can be used for multiple links as long as they are in different cells
- Mobile devices use less power than with a single transmitter or satellite since the cell towers are closer
- Larger coverage area than a single terrestrial transmitter, since additional cell towers can be added indefinitely and are not limited by the horizon

Major telecommunications providers have deployed voice and data cellular networks over most of the inhabited land area of the Earth. This allows mobile phones and mobile computing devices to be connected to the public switched telephone network and public Internet. Private cellular networks can be used for research or for large organizations and fleets, such as dispatch for local public safety agencies or a taxicab company.



Top of a cellular radio tower

## Concept




Example of frequency reuse factor or pattern 1/4

In a cellular radio system, a land area to be supplied with radio service is divided into regular shaped cells, which can be hexagonal, square, circular or some other regular shapes, although hexagonal cells are conventional. Each of these cells is assigned with multiple frequencies ($f_1 - f_6$) which have corresponding radio base stations. The group of frequencies can be reused in other cells, provided that the same frequencies are not reused in adjacent neighboring cells as that would cause co-channel interference.

The increased capacity in a cellular network, compared with a network with a single transmitter, comes from the mobile communication switching system developed by Amos Joel of Bell Labs that permitted multiple callers in the same area to use the same frequency by switching calls made using the same frequency to the nearest available cellular tower having that frequency available and from the fact that the same radio frequency can be reused in a different area for a completely different transmission. If there is a single plain transmitter, only one transmission can be used on any given frequency. Unfortunately, there is inevitably some level of interference from the signal from the other cells which use the same frequency. This means that, in a standard FDMA system, there must be at least a one cell gap between cells which reuse the same frequency.

In the simple case of the taxi company, each radio had a manually operated channel selector knob to tune to different frequencies. As the drivers moved around, they would change from channel to channel. The drivers knew which frequency covered approximately what area. When they did not receive a signal from the transmitter, they would try other channels until they found one that worked. The taxi drivers would only speak one at a time, when invited by the base station operator (this is, in a sense, time division multiple access (TDMA)).

## Cell Signal Encoding

To distinguish signals from several different transmitters, time division multiple access (TDMA), frequency division multiple access (FDMA), code division multiple access (CDMA), and orthogonal frequency division multiple access (OFDMA) were developed.

With TDMA, the transmitting and receiving time slots used by different users in each cell are different from each other.

With FDMA, the transmitting and receiving frequencies used by different users in each cell are different from each other. In a simple taxi system, the taxi driver manually tuned to a frequency of a chosen cell to obtain a strong signal and to avoid interference from signals from other cells.

The principle of CDMA is more complex, but achieves the same result; the distributed transceivers can select one cell and listen to it.

Other available methods of multiplexing such as polarization division multiple access (PDMA) cannot be used to separate signals from one cell to the next since the effects of both vary with position and this would make signal separation practically impossible. Time division multiple access is used in combination with either FDMA or CDMA in a number of systems to give multiple channels within the coverage area of a single cell.

## Frequency Reuse

The key characteristic of a cellular network is the ability to re-use frequencies to increase both coverage and capacity. As described above, adjacent cells must use different frequencies, however there is no problem with two cells sufficiently far apart operating on the same frequency, provided the masts and cellular network users' equipment do not transmit with too much power.

The elements that determine frequency reuse are the reuse distance and the reuse factor. The reuse distance, $D$ is calculated as

$$D = R\sqrt{3N},$$

where $R$ is the cell radius and $N$ is the number of cells per cluster. Cells may vary in radius from 1 to 30 kilometres (0.62 to 18.64 mi). The boundaries of the cells can also overlap between adjacent cells and large cells can be divided into smaller cells.

The frequency reuse factor is the rate at which the same frequency can be used in the network. It is *1/K* (or *K* according to some books) where *K* is the number of cells which cannot use the same frequencies for transmission. Common values for the frequency reuse factor are 1/3, 1/4, 1/7, 1/9 and 1/12 (or 3, 4, 7, 9 and 12 depending on notation).

In case of *N* sector antennas on the same base station site, each with different direction, the base station site can serve N different sectors. *N* is typically 3. A **reuse pattern** of *N/K* denotes a further division in frequency among *N* sector antennas per site. Some current and historical reuse patterns are 3/7 (North American AMPS), 6/4 (Motorola NAMPS), and 3/4 (GSM).

If the total available bandwidth is *B*, each cell can only use a number of frequency channels corresponding to a bandwidth of *B/K*, and each sector can use a bandwidth of *B/NK*.

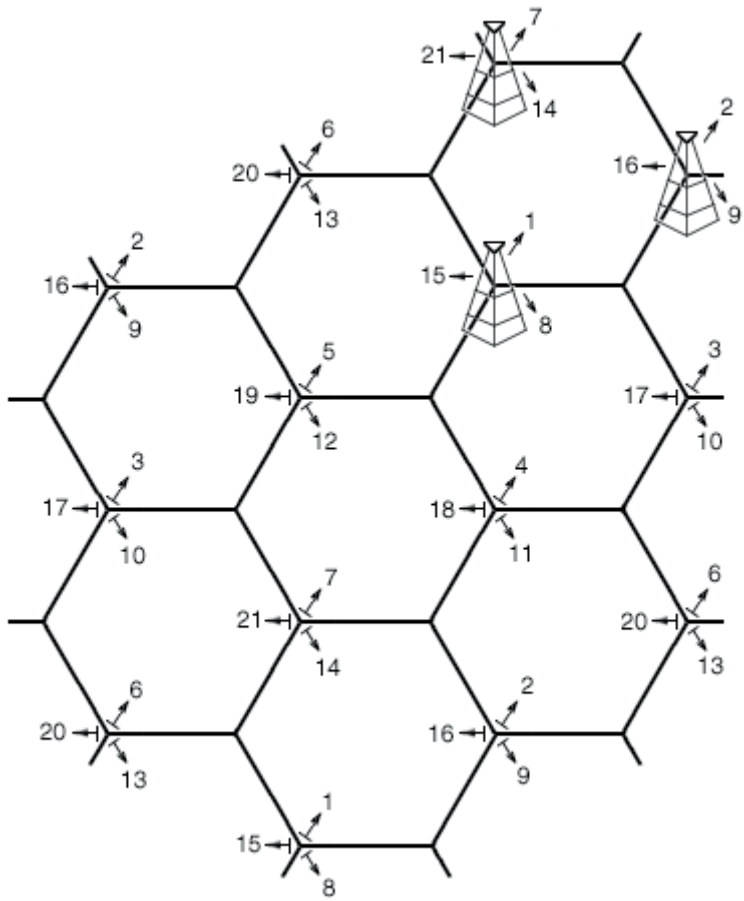
Code division multiple access-based systems use a wider frequency band to achieve the same rate of transmission as FDMA, but this is compensated for by the ability to use a frequency reuse factor of 1, for example using a reuse pattern of 1/1. In other words, adjacent base station sites use the same frequencies, and the different base stations and users are separated by codes rather than frequencies. While *N* is shown as 1 in this example, that does not mean the CDMA cell has only one sector, but rather that the entire cell bandwidth is also available to each sector individually.

Depending on the size of the city, a taxi system may not have any frequency-reuse in its own city, but certainly in other nearby cities, the same frequency can be used. In a large city, on the other hand, frequency-reuse could certainly be in use.

Recently also orthogonal frequency-division multiple access based systems such as LTE are being deployed with a frequency reuse of 1. Since such systems do not spread the signal across the frequency band, inter-cell radio resource management is important to coordinate resource allocation between different cell sites and to limit the inter-cell interference. There are various means of Inter-Cell Interference Coordination (ICIC)

already defined in the standard. Coordinated scheduling, multi-site MIMO or multi-site beam forming are other examples for inter-cell radio resource management that might be standardized in the future.

## Directional Antennas




Cellular telephone frequency reuse pattern. See U.S. Patent 4,144,411

Cell towers frequently use a directional signal to improve reception in higher-traffic areas. In the United States, the FCC limits omnidirectional cell tower signals to 100 watts of power. If the tower has directional antennas, the FCC allows the cell operator to broadcast up to 500 watts of effective radiated power (ERP).

Cell phone companies use this directional signal to improve reception along highways and inside buildings like stadiums and arenas. As a result, a cell phone user may be standing in sight of a cell tower, but still have trouble getting a good signal because the directional antennas point in a different direction.

Although the original cell towers created an even, omnidirectional signal, were at the centers of the cells and were omnidirectional, a cellular map can be redrawn with the cellular telephone towers located at the corners of the hexagons where three cells converge. Each tower has three sets of directional antennas aimed in three different directions with 120 degrees for each cell (totaling 360 degrees) and receiving/transmitting into three different cells at different frequencies. This provides a minimum of three channels, and three towers for each cell and greatly increases the chances of receiving a usable signal from at least one direction.

The numbers in the illustration are channel numbers, which repeat every 3 cells. Large cells can be subdivided into smaller cells for high volume areas.

### *Broadcast Messages and Paging*

Practically every cellular system has some kind of broadcast mechanism. This can be used directly for distributing information to multiple mobiles. Commonly, for example in mobile telephony systems, the most important use of broadcast information is to set up channels for one-to-one communication between the mobile transceiver and the base station. This is called **paging**. The three different paging procedures generally adopted are sequential, parallel and selective paging.

The details of the process of paging vary somewhat from network to network, but normally we know a limited number of cells where the phone is located (this group of cells is called a Location Area in the GSM or UMTS system, or Routing Area if a data packet session is involved; in LTE, cells are grouped into Tracking Areas). Paging takes place by sending the broadcast message to all of those cells. Paging messages can be used for information transfer. This happens in pagers, in CDMA systems for sending SMS messages, and in the UMTS system where it allows for low downlink latency in packet-based connections.

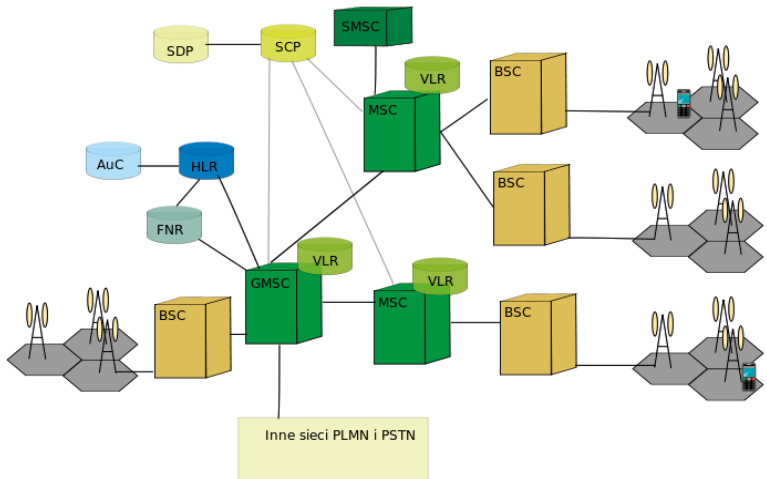
## Movement from Cell to Cell and Handing Over

In a primitive taxi system, when the taxi moved away from a first tower and closer to a second tower, the taxi driver manually switched from one frequency to another as needed. If a communication was interrupted due to a loss of a signal, the taxi driver asked the base station operator to repeat the message on a different frequency.

In a cellular system, as the distributed mobile transceivers move from cell to cell during an ongoing continuous communication, switching from one cell frequency to a different cell frequency is done electronically without interruption and without a base station operator or manual switching. This is called the handover or handoff. Typically, a new channel is automatically selected for the mobile unit on the new base station which will serve it. The mobile unit then automatically switches from the current channel to the new channel and communication continues.

The exact details of the mobile system's move from one base station to the other varies considerably from system to system (see the example below for how a mobile phone network manages handover).

## Mobile Phone Network




GSM network architecture

The most common example of a cellular network is a mobile phone (cell phone) network. A mobile phone is a portable telephone which receives or makes calls through a cell site (base station), or transmitting tower. Radio waves are used to transfer signals to and from the cell phone.

Modern mobile phone networks use cells because radio frequencies are a limited, shared resource. Cell-sites and handsets change frequency under computer control and use low power transmitters so that the usually limited number of radio frequencies can be simultaneously used by many callers with less interference.

A cellular network is used by the mobile phone operator to achieve both coverage and capacity for their subscribers. Large geographic areas are split into smaller cells to avoid line-of-sight signal loss and to support a large number of active phones in that area. All of the cell sites are connected to telephone exchanges (or switches), which in turn connect to the public telephone network.

In cities, each cell site may have a range of up to approximately ½ mile (0.80 km), while in rural areas, the range could be as much as 5 miles (8.0 km). It is possible that in clear open areas, a user may receive signals from a cell site 25 miles (40 km) away.

Since almost all mobile phones use cellular technology, including GSM, CDMA, and AMPS (analog), the term “cell phone” is in some regions, notably the US, used interchangeably with “mobile phone”. However, satellite phones are mobile phones that do not communicate directly with a ground-based cellular tower, but may do so indirectly by way of a satellite.

There are a number of different digital cellular technologies, including: Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), cdmaOne, CDMA2000, Evolution-Data Optimized (EV-DO), Enhanced Data Rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), Digital Enhanced Cordless Telecommunications (DECT), Digital AMPS (IS-136/TDMA), and Integrated Digital Enhanced Network (iDEN). The transition from existing analog to the digital standard followed a very different path in Europe and the US. As a consequence, multiple digital standards surfaced in the US, while Europe and many countries converged towards the GSM standard.

## Structure of the Mobile Phone Cellular Network

A simple view of the cellular mobile-radio network consists of the following:

- A network of radio base stations forming the base station subsystem.
- The core circuit switched network for handling voice calls and text
- A packet switched network for handling mobile data
- The public switched telephone network to connect subscribers to the wider telephony network

This network is the foundation of the GSM system network. There are many functions that are performed by this network in order to make sure customers get the desired service including mobility management, registration, call set-up, and handover.

Any phone connects to the network via an RBS (Radio Base Station) at a corner of the corresponding cell which in turn connects to the Mobile switching center (MSC). The MSC provides a connection to the public switched telephone network (PSTN). The link from a phone to the RBS is called an *uplink* while the other way is termed *downlink*.

Radio channels effectively use the transmission medium through the use of the following multiplexing and access schemes: frequency division multiple access (FDMA), time division multiple access (TDMA), code division multiple access (CDMA), and space division multiple access (SDMA).

## Small Cells

Small cells, which have a smaller coverage area than base stations, are categorised as follows:

- Microcell, less than 2 kilometres
- Picocell, less than 200 metres
- Femtocell, around 10 metres

## Cellular Handover in Mobile Phone Networks

As the phone user moves from one cell area to another cell while a call is in progress, the mobile station will search for a new channel to attach to in order not to drop the

call. Once a new channel is found, the network will command the mobile unit to switch to the new channel and at the same time switch the call onto the new channel.

With CDMA, multiple CDMA handsets share a specific radio channel. The signals are separated by using a pseudonoise code (PN code) specific to each phone. As the user moves from one cell to another, the handset sets up radio links with multiple cell sites (or sectors of the same site) simultaneously. This is known as "soft handoff" because, unlike with traditional cellular technology, there is no one defined point where the phone switches to the new cell.

In IS-95 inter-frequency handovers and older analog systems such as NMT it will typically be impossible to test the target channel directly while communicating. In this case other techniques have to be used such as pilot beacons in IS-95. This means that there is almost always a brief break in the communication while searching for the new channel followed by the risk of an unexpected return to the old channel.

If there is no ongoing communication or the communication can be interrupted, it is possible for the mobile unit to spontaneously move from one cell to another and then notify the base station with the strongest signal.

## *Cellular Frequency Choice in Mobile Phone Networks*

The effect of frequency on cell coverage means that different frequencies serve better for different uses. Low frequencies, such as 450 MHz NMT, serve very well for countryside coverage. GSM 900 (900 MHz) is a suitable solution for light urban coverage. GSM 1800 (1.8 GHz) starts to be limited by structural walls. UMTS, at 2.1 GHz is quite similar in coverage to GSM 1800.

Higher frequencies are a disadvantage when it comes to coverage, but it is a decided advantage when it comes to capacity. Pico cells, covering e.g. one floor of a building, become possible, and the same frequency can be used for cells which are practically neighbours.

Cell service area may also vary due to interference from transmitting systems, both within and around that cell. This is true especially in CDMA based systems. The receiver requires a certain signal-to-noise ratio, and the transmitter should not send with too high transmission power in view to not cause interference with other transmitters. As the receiver moves away from the transmitter, the power received decreases, so the power control algorithm of the transmitter increases the power it transmits to restore the level of received power. As the interference (noise) rises above the received power from the transmitter, and the power of the transmitter cannot be increased any more, the signal becomes corrupted and eventually unusable. In CDMA-based systems, the effect of interference from other mobile transmitters in the same cell on coverage area is very marked and has a special name, *cell breathing*.

One can see examples of cell coverage by studying some of the coverage maps provided by real operators on their web sites or by looking at independently crowdsourced maps such as OpenSignal. In certain cases they may mark the site of the transmitter, in others it can be calculated by working out the point of strongest coverage.

A cellular repeater is used to extend cell coverage into larger areas. They range from wideband repeaters for consumer use in homes and offices to smart or digital repeaters for industrial needs.

### *Coverage Comparison of Different Frequencies*

The following table shows the dependency of the coverage area of one cell on the frequency of a CDMA2000 network:

| Frequency (MHz) | Cell radius (km) | Cell area (km2) | Relative Cell Count |
|---|---|---|---|
| 450 | 48.9 | 7521 | 1 |
| 950 | 26.9 | 2269 | 3.3 |
| 1800 | 14.0 | 618 | 12.2 |
| 2100 | 12.0 | 449 | 16.2 |

## CYCLADES

The CYCLADES computer network (French pronunciation: [siklad]) was a French research network created in the early 1970s. It was one of the pioneering networks experimenting with the concept of packet switching, and was developed to explore alternatives to the ARPANET design. It supported general local network research.

The CYCLADES network was the first to make the hosts responsible for the reliable delivery of data, rather than this being a centralized service of the network itself. Datagrams were exchanged on the network using transport protocols that do not guarantee reliable delivery, but only attempt best-effort. To empower the network leaves, the hosts, to perform error-correction, the network ensured end-to-end protocol transparency, a concept later to be known as the end-to-end principle. This simplified network design, reduced network latency, and reduced the opportunities for single point failures. The experience with these concepts led to the design of key features of the Internet protocol in the ARPANET project.

The network was sponsored by the French government, through the Institut de Recherche en lnformatique et en Automatique (IRIA), the national research laboratory for computer science in France, now known as INRIA, which served as the co-ordinating agency. Several French computer manufacturers, research institutes and universities contributed to the effort. CYCLADES was designed and directed by Louis Pouzin.

## Conception and Deployment

Design and staffing started in 1972, and November 1973 saw the first demonstration, using three hosts and one packet switch. Deployment continued in 1974, with three packet switches installed by February, although at that point the network was only operational for three hours each day. By June the network was up to seven switches, and was available throughout the day for experimental use.

A terminal concentrator was also developed that year, since time-sharing was still a prevalent mode of computer use. In 1975, the network shrank slightly due to budgetary constraints, but the setback was only temporary. At that point, the network provided remote login, remote batch and file transfer user application services.

By 1976 the network was in full deployment, eventually numbering 20 nodes with connections to NPL in London, ESA in Rome, and to the European Informatics Network (EIN).

## Technical Details

CYCLADES used a layered architecture, as did the Internet. The basic packet transmission like function, named CIGALE, was novel; however, it provided an unreliable *datagram* service (the word was coined by Louis Pouzin by combining *data* and *telegram*). Since the packet switches no longer had to ensure correct delivery of data, this greatly simplified their design.

"The inspiration for datagrams had two sources. One was Donald Davies' studies. He had done some simulation of datagram networks, although he had not built any, and it looked technically viable. The second inspiration was I like things simple. I didn't see any real technical motivation to overlay two levels of end-to-end protocols. I thought one was enough."

—Louis Pouzin

The CIGALE network featured a distance vector routing protocol, and allowed experimentation with various metrics. it also included a time synchronization protocol in all the packet switches. CIGALE included early attempts at performing congestion control by dropping excess packets.

The name CIGALE—(French pronunciation: which is French for *cicada*—originates from the fact that the developers installed a speaker at each computer, so that "it went 'chirp chirp chirp' like cicadas" when a packet passed a computer.

An end-to-end protocol built on top of that provided a reliable transport service, on top of which applications were built. It provided a reliable sequence of user-visible data units called *letters*, rather than the reliable byte stream of TCP. The transport protocol was able to deal with out-of-order and unreliable delivery of datagrams, using the now-standard mechanisms of end-end acknowledgments and timeouts; it also featured sliding windows and end-to-end flow control.

## Demise

By 1976, the French PTT was developing Transpac, a packet network based on the emerging X.25 standard. The academic debates between datagram and virtual circuit networks continued for some time, but were eventually cut short by bureaucratic decisions.

Data transmission was a state monopoly in France at the time, and IRIA needed a special dispensation to run the CYCLADES network. The PTT did not agree to funding by the government of a competitor to their Transpac network, and insisted that the permission and funding be rescinded. By 1981, Cyclades was forced to shut down.

## Legacy

The most important legacy of CYCLADES was in showing that moving the responsibility for reliability into the hosts was workable, and produced a well-functioning service network. It also showed that it greatly reduced the complexity of the packet switches. The concept became a cornerstone in the design of the Internet.

The network was also a fertile ground for experimentation, and allowed a generation of French computer scientists to experiment with networking concepts. Louis Pouzin and the CYCLADES alumni initiated a number of follow-on projects at IRIA to experiment with local area networks, satellite networks, the Unix operating system, and the message passing operating system Chorus.

Hubert Zimmermann used his experience in CYCLADES to influence the design of the OSI model, which is still a common pedagogical tool.

CYCLADES alumni and researchers at IRIA/INRIA were also influential in spreading adoption of the Internet in France, eventually witnessing the success of the datagram-based Internet, and the demise of the X.25 and ATM virtual circuit networks.

## REFERENCES


9. Guowang Miao; Jens Zander; Ki Won Sung; Ben Slimane (2016). Fundamentals of Mobile Data Networks. Cambridge University Press. ISBN 1107143217.
10. Tom Simonite January 24, 2013 (2013-01-24). "Google's Private Cell Phone Network Could Be a Threat to Cellular Carriers | MIT Technology Review". Technologyreview.com. Retrieved 2013-11-23.
11. "Be Mobile, Stay Connected | PMN". Privatemobilenetworks.com. Retrieved 2013-11-23.
12. U.S. Patent 3,663,762, issued May 16, 1972.
13. J. E. Flood. Telecommunication Networks. Institution of Electrical Engineers, London, UK, 1997. chapter 12.
14. "Phone Networks". The Reverse Phone. 8 June 2011. Retrieved 2 April 2012.
15. Pauli, Volker; Naranjo, Juan Diego; Seidel, Eiko (December 2010). "Heterogeneous LTE Networks and Inter-Cell Interference Coordination" (PDF). Nomor Research. Retrieved 2 April 2012.
16. Drucker, Elliott, The Myth of Cellular Tower Health Hazards, retrieved 2013-11-19
17. "Cellular Telephone Basics". Privateline.com. 1 January 2006. p. 2. Retrieved 2 April 2012.
18. U.S. Patent 4,144,411 – Cellular Radiotelephone System for Different Cell Sizes – Richard H. Frenkiel (Bell Labs), filed Sep 22, 1976, issued March 13, 1979
19. Paetsch, Michael (1993): The evolution of mobile communications in the US and Europe. Regulation, technology, and markets. Boston, London: Artech House (The Artech House mobile communications library).
20. page 17

21. L.A Lievrouw - Handbook of New Media: Student Edition (p.253)(edited by L.A Lievrouw, S.M. Livingstone), published by SAGE 2006 (abridged, reprint, revised), 475 pages, ISBN 1412918731 [Retrieved 2015-08-15]
22. G. Schneider; J. Evans; K. Pinard. The Internet - Illustrated. published by Cengage Learning 26 Oct 2009, 296 pages, ISBN 0538750987, Available Titles Skills Assessment Manager (SAM) - Office 2010 Series Illustrated (Course Technology). Retrieved 2015-08-15.
23. K.G. Coffman & A.M. Odlyzco - Optical Fiber Telecommunications IV-B: Systems and Impairments published by Academic Press 22 May 2002, 1022 pages, Optics and Photonics, ISBN 0080513190, (edited by I. Kaminow & T. Li) [Retrieved 2015-08-15]
24. R. Oppliger. Internet and Intranet Security (p.12). Artech House, 1 Jan 2001, 403 pages, Artech House computer security series, ISBN 1580531660. Retrieved 2015-08-15.
25. (ed. by H. Bidgoli). The Internet Encyclopedia, G Â– O. published by John Wiley & Sons 11 May 2004, 840 pages, ISBN 0471689963, Volume 2 of The Internet Encyclopedia. Retrieved 2015-08-15.
26. "Lawrence Roberts Manages The ARPANET Program". Living Internet.com. Retrieved 6 November 2008.
27. "Packet Switching History", Living Internet, retrieved 26 August 2012
28. "J.C.R. Licklider And The Universal Network", Living Internet
29. "IPTO – Information Processing Techniques Office", Living Internet
30. John Markoff (20 December 1999). "An Internet Pioneer Ponders the Next Revolution". The New York Times. Archived from the original on 22 September 2008. Retrieved 20 September 2008.
31. "Paul Baran and the Origins of the Internet". RAND corporation. Retrieved 29 March 2011.
32. Scantlebury, Roger (25 June 2013). "Internet pioneers airbrushed from history". The Guardian. Retrieved 1 August 2015.
33. "Packets of data were the key...". NPL. Retrieved 1 August 2015.
34. Isaacson, Walter (2014). The Innovators: How a Group of Hackers, Geniuses, and Geeks Created the Digital Revolution. Simon & Schuster. p. 237. ISBN 9781476708690.
35. "The accelerator of the modern age". BBC News. 5 August 2008. Retrieved 19 May 2009.
36. Cambell-Kelly, Martin (Autumn 2008). "Pioneer Profiles: Donald Davies". Computer Resurrection (44). ISSN 0958-7403.
37. Roberts, Lawrence G. (November 1978). "The Evolution of Packet Switching". Retrieved 9 April 2016.
38. "Donald Davies". thocp.net; "Donald Davies". internethalloffame.org.
39. C. Hempstead; W. Worthington. Encyclopedia of 20th-Century Technology.

Routledge 8 Aug 2005, 992 pages, (edited by C. Hempstead, W. Worthington),. Retrieved 2015-08-15.(source: Gatlinburg, ... Association for Computing Machinery)

40. M. Ziewitz & I. Brown (2013). Research Handbook on Governance of the Internet. Edward Elgar Publishing. p. 7. ISBN 1849805040. Retrieved 2015-08-16.
41. "Brief History of the Internet". Internet Society. Retrieved April 9, 2016.
42. "IMP – Interface Message Processor", Living Internet
43. Wise, Adrian. "Honeywell DDP-516". Old-Computers.com. Retrieved 21 September 2008.
44. "A Brief History of the Internet". Internet Society. Archived from the original on 18 September 2008. Retrieved 20 September 2008.
45. Brand, Stewart (March 2001). "Founding Father". Wired (9.03). Retrieved 31 December 2011.
46. "Shapiro: Computer Network Meeting of October 9-10, 1967". stanford.edu.
47. Lukasik, Stephen J. (2011). "Why the Arpanet Was Built". IEEE Annals of the History of Computing. 33 (3): 4–20. doi:10.1109/MAHC.2010.11.
48. "Charles Herzfeld on ARPANET and Computers". About.com. Retrieved 21 December 2008.
49. Janet Abbate (2000) Inventing the Internet pp.194-5
50. Vernon W. Ruttan (2005) Is War Necessary for Economic Growth?p.125
51. "ARPANET – The First Internet", Living Internet
52. Jessica Savio (1 April 2011). "Browsing history: A heritage site has been set up in Boelter Hall 3420, the room the first Internet message originated in". Daily Bruin. UCLA.
53. Chris Sutton (2 September 2004). "Internet Began 35 Years Ago at UCLA with First Message Ever Sent Between Two Computers". UCLA. Archived from the original on 8 March 2008.
54. "NORSAR and the Internet". NORSAR (Norway Seismic Array Research). Retrieved 25 August 2012.
55. DEFENSE DATA NETWORK NEWSLETTER DDN-NEWS 26, 6 May 1983
56. ARPANET INFORMATION BROCHURE (NIC 50003) Defense Communications Agency, December 1985.
57. Fritz E. Froehlich; Allen Kent (1990). "ARPANET, the Defense Data Network, and Internet". The Froehlich/Kent Encyclopedia of Telecommunications. 1. CRC Press. pp. 341–375. ISBN 978-0-8247-2900-4.
58. Stacy, Christopher C. (7 September 1982). Getting Started Computing at the AI Lab. AI Lab, Massachusetts Institute of Technology. p. 9.
59. Kirstein, Peter T. (July–September 2009). "The Early Days of the Arpanet". IEEE Annals of the History of Computing. 31 (3): 67. doi:10.1109/mahc.2009.35. ISSN 1058-6180.

60. "NCP – Network Control Program", Living Internet
61. "TCP/IP Internet Protocol", Living Internet
62. "NSFNET – National Science Foundation Network", Living Internet
63. "Digital Communication".
64. "III". A History of the ARPANET: The First Decade (PDF) (Report). Arlington, VA: Bolt, Beranek & Newman Inc. 1 April 1981. p. 132. section 2.3.4
65. Abbate, Janet (11 June 1999). Inventing the Internet. Cambridge, MA: MIT Press. ASIN B003VPWY6E. ISBN 0-262-01172-7.
66. "Milestones:Birthplace of the Internet, 1969". IEEE Global History Network. IEEE. Retrieved 4 August 2011.
67. "Milestones:Inception of the ARPANET, 1969". IEEE Global History Network. IEEE. Retrieved 4 August 2011.
68. Interface Message Processor: Specifications for the Interconnection of a Host and an IMP, Report No. 1822, Bolt Beranek and Newman, Inc. (BBN)
69. Tomlinson, Ray. "The First Network Email". BBN. Retrieved 6 March 2012.
70. Steven King (Producer), Peter Chvany (Director/Editor) (1972). Computer Networks: The Heralds of Resource Sharing. Retrieved 20 December 2011.
71. "Scenario", Benson, Season 6, Episode 132 of 158, American Broadcasting Company (ABC), Witt/Thomas/Harris Productions, 22 February 1985
72. The X-Files Season 5, Ep. 3 "Unusual Suspects".[better source needed]
73. Season 2, Episode 11 "2πR"
74. Season 3, Episode 12 "Aletheia"
75. "BBC News - SCI/TECH - Hacking: A history". bbc.co.uk.
76. "Hobbes' Internet Timeline - the definitive ARPAnet & Internet history". zakon.org.
77. CREN. "A Brief History of "Bit.net"". Retrieved August 30, 2012.
78. Cailliau, Robert; Gillies, James (1 January 2000). How the Web Was Born: The Story of the World Wide Web. San Val, Incorporated. pp. 74, 75. ISBN 978-0-613-92163-3.
79. Hura, Gurdeep (28 March 2001). Data and Computer Communications: Networking and Internetworking. CRC Press. p. 779. ISBN 9780849309281.
80. http://dhhumanist.org/Archives/Virginia/v04/1140.html
81. http://gadgets.ndtv.com/internet/news/as-emails-turn-40-scientists-recall-india-arrival-277436

CHAPTER 8

# Telecommunications Equipment

## Chapter Contents


- **Introduction**
- **Analogue Switch**
- **Transmission Line**
- **Modem**
- **Router (Computing)**


Telecommunications equipment refers to hardware used mainly for telecommunications such as transmission lines, multiplexers and base transceiver stations. It encompasses different types of communication technologies including telephones, radios and even computers. Since the early 1990s, the line between telecommunications equipment and IT equipment has started to blur as the growth of the Internet has resulted in the increasing importance of telecommunications infrastructure for data transfer.

## INTRODUCTION

Telecommunications equipment (also telecoms equipment or communications equipment) is hardware used for the purposes of telecommunications. Since the 1990s the boundary between telecoms equipment and IT hardware has become blurred as a result of the growth of the internet and its increasing role in the transfer of telecoms data.

### Types

Telecommunications equipment can be broadly broken down into the following categories:

- Public switching equipment

- Analogue switches
- Digital switches

■ Transmission equipment
- Transmission lines
- Optical fiber
- Base transceiver stations
- Multiplexers
- Local loops
- Communications satellites

■ Customer premises equipment
- Private switches
- Local area networks
- Modems
- Mobile phones
- Landline telephones
- Answering machines
- Teleprinters
- Fax machines
- Pagers
- Routers

## ANALOGUE SWITCH

The analogue (or analog) switch, also called the bilateral switch, is an electronic component that behaves in a similar way to a relay, but has no moving parts. The switching element is normally a pair of MOSFET transistors, one an N-channel device, the other a P-channel device. The device can conduct analog or digital signals in either direction when on and isolates the switched terminals when off. Analogue switches are usually manufactured as integrated circuits in packages containing multiple switches (typically two, four or eight). These include the 4016 and 4066 from the 4000 series.

The control input to the device may be a signal that switches between the positive and negative supply voltages, with the more positive voltage switching the device on and the more negative switching the device off. Other circuits are designed to communicate through a serial port with a host controller in order to set switches on or off.

The signal being switched must remain within the bounds of the positive and negative supply rails which are connected to the P-MOS and N-MOS body terminals. The switch generally provides good isolation between the control signal and the input/output signals. They are not used for high voltage switching.

Important parameters of an analogue switch are:

- on-resistance: the resistance when switched on. This commonly ranges from 5 ohms to a few hundred ohms.
- off-resistance: the resistance when switched off. This is typically a number of megohms or gigaohms.
- signal range: the minimum and maximum voltages allowed for the signal to be passed through. If these are exceeded, the switch may be destroyed by excessive currents. Older types of switches can even *latch up*, which means that they continue to conduct excessive currents even after the faulty signal is removed.
- charge injection. This effect causes the switch to inject a small electric charge into the signal when it switches on, causing a small spike or glitch. The charge injection is specified in coulombs.

Analogue switches are available in both through-hole technology or by surface-mount technology packages.

# TRANSMISSION LINE

In communications and electronic engineering, a transmission line is a specialized cable or other structure designed to carry alternating current of radio frequency, that is, currents with a frequency high enough that their wave nature must be taken into account. Transmission lines are used for purposes such as connecting radio transmitters and receivers with their antennas, distributing cable television signals, trunklines routing calls between telephone switching centres, computer network connections and high speed computer data buses.

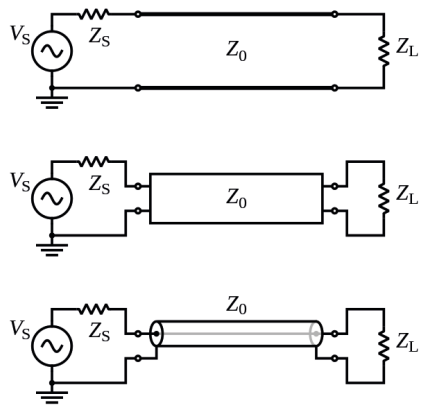
This article covers two-conductor transmission line such as parallel line (ladder line), coaxial cable, stripline, and microstrip. Some sources also refer to waveguide, dielectric waveguide, and even optical fibre as transmission line, however these lines require different analytical techniques and so are not covered by this article; see Waveguide (electromagnetism).

## Applicability

In many electric circuits, the length of the wires connecting the components can for the most part be ignored. That is, the voltage on the wire at a given time can be assumed to be the same at all points. However, when the voltage changes in a time interval comparable to the time it takes for the signal to travel down the wire, the length becomes important and the wire must be treated as a transmission line. Stated another way, the length of the wire is important when the signal includes frequency components with corresponding wavelengths comparable to or less than the length of the wire.

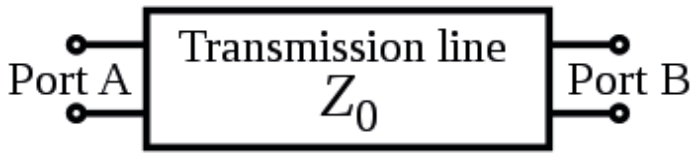
A common rule of thumb is that the cable or wire should be treated as a transmission line if the length is greater than 1/10 of the wavelength. At this length the phase delay and the interference of any reflections on the line become important and can lead to unpredictable behaviour in systems which have not been carefully designed using transmission line theory.

## The Four Terminal Model




Variations on the schematicelectronic symbol for a transmission line.

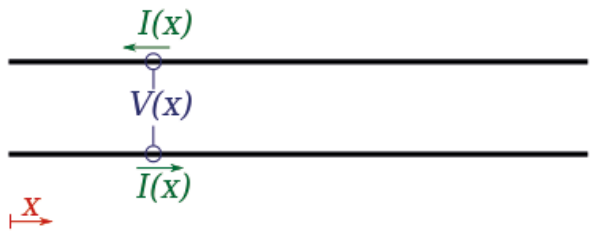
For the purposes of analysis, an electrical transmission line can be modelled as a two-port network (also called a quadripole), as follows:




In the simplest case, the network is assumed to be linear (i.e. the complex voltage across either port is proportional to the complex current flowing into it when there are no reflections), and the two ports are assumed to be interchangeable. If the transmission line is uniform along its length, then its behaviour is largely described by a single parameter called the *characteristic impedance*, symbol $Z_0$. This is the ratio of the complex voltage of a given wave to the complex current of the same wave at any point on the line. Typical values of $Z_0$ are 50 or 75 ohms for a coaxial cable, about 100 ohms for a twisted pair of wires, and about 300 ohms for a common type of untwisted pair used in radio transmission.

When sending power down a transmission line, it is usually desirable that as much power as possible will be absorbed by the load and as little as possible will be reflected back to the source. This can be ensured by making the load impedance equal to $Z_0$, in which case the transmission line is said to be *matched*.

A transmission line is drawn as two black wires. At a distance $x$ into the line, there is current $I(x)$ travelling through each wire, and there is a voltage difference $V(x)$ between the wires. If the current and voltage come from a single wave (with no reflection), then $V(x) / I(x) = Z_0$, where $Z_0$ is the *characteristic impedance* of the line.




Some of the power that is fed into a transmission line is lost because of its resistance. This effect is called *ohmic* or *resistive* loss (see ohmic heating). At high frequencies, another effect called *dielectric loss* becomes significant, adding to the losses caused by resistance. Dielectric loss is caused when the insulating material inside the transmission line absorbs energy from the alternating electric field and converts it to heat (see dielectric heating). The transmission line is modelled with a resistance (R) and inductance (L) in series with a capacitance (C) and conductance (G) in parallel. The resistance and conductance contribute to the loss in a transmission line.

The total loss of power in a transmission line is often specified in decibels per metre (dB/m), and usually depends on the frequency of the signal. The manufacturer often supplies a chart showing the loss in dB/m at a range of frequencies. A loss of 3 dB corresponds approximately to a halving of the power.

High-frequency transmission lines can be defined as those designed to carry electromagnetic waves whose wavelengths are shorter than or comparable to the length of the line. Under these conditions, the approximations useful for calculations at lower frequencies are no longer accurate. This often occurs with radio, microwave and optical signals, metal mesh optical filters, and with the signals found in high-speed digital circuits.

## Communications satellite

A communications satellite is an artificial satellite that relays and amplifies radio telecommunications signals via a transponder; it creates a communication channel between a source transmitter and a receiver at different locations on Earth. Communications satellites are used for television, telephone, radio, internet, and military applications. There are over 2,000 communications satellites in Earth's orbit, used by both private and government organizations.

Wireless communication uses electromagnetic waves to carry signals. These waves require line-of-sight, and are thus obstructed by the curvature of the Earth. The purpose of communications satellites is to relay the signal around the curve of the Earth allowing communication between widely separated points. Communications satellites use a wide range of radio and microwave frequencies. To avoid signal interference, international organizations have regulations for which frequency ranges or "bands" certain organizations are allowed to use. This allocation of bands minimizes the risk of signal interference.

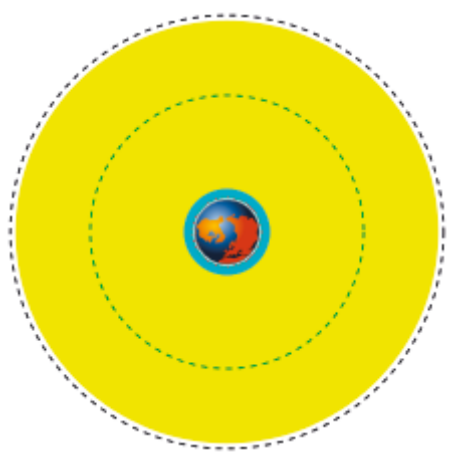
## Satellite Orbits

Communications satellites usually have one of three primary types of orbit, while other orbital classifications are used to further specify orbital details.

- Geostationary satellites have a *geostationary orbit* (GEO), which is 35,786 kilometres (22,236 mi) from Earth's surface. This orbit has the special characteristic that the apparent position of the satellite in the sky when viewed by a ground observer does not change, the satellite appears to "stand still" in the sky. This is because the satellite's orbital period is the same as the rotation rate of the Earth. The advantage of this orbit is that ground antennas do not have to track the satellite across the sky, they can be fixed to point at the location in the sky the satellite appears.
- *Medium Earth orbit* (MEO) satellites are closer to Earth. Orbital altitudes range from 2,000 to 35,786 kilometres (1,243 to 22,236 mi) above Earth.
- The region below medium orbits is referred to as *low Earth orbit* (LEO), and is about 160 to 2,000 kilometres (99 to 1,243 mi) above Earth.

As satellites in MEO and LEO orbit the Earth faster, they do not remain visible in the sky to a fixed point on Earth continually like a geostationary satellite, but appear to a ground observer to cross the sky and "set" when they go behind the Earth. Therefore, to provide continuous communications capability with these lower orbits requires a larger number of satellites, so one will always be in the sky for transmission of communication signals. However, due to their relatively small distance to the Earth their signals are stronger.

### *Low Earth Orbiting (LEO) Satellites*



Low Earth orbit in Cyan

A low Earth orbit (LEO) typically is a circular orbit about 160 to 2,000 kilometres (99 to 1,243 mi) above the earth's surface and, correspondingly, a period (time to revolve around the earth) of about 90 minutes.

Because of their low altitude, these satellites are only visible from within a radius of roughly 1,000 kilometres (620 mi) from the sub-satellite point. In addition, satellites in low earth orbit change their position relative to the ground position quickly. So even for local applications, a large number of satellites are needed if the mission requires uninterrupted connectivity.

Low-Earth-orbiting satellites are less expensive to launch into orbit than geostationary satellites and, due to proximity to the ground, do not require as high signal strength (*Recall that signal strength falls off as the square of the distance from the source, so the effect is dramatic)*. Thus there is a trade off between the number of satellites and their cost.

In addition, there are important differences in the onboard and ground equipment needed to support the two types of missions.

## Satellite Constellation

A group of satellites working in concert is known as a satellite constellation. Two such constellations, intended to provide satellite phone services, primarily to remote areas, are the Iridium and Globalstar systems. The Iridium system has 66 satellites.

It is also possible to offer discontinuous coverage using a low-Earth-orbit satellite capable of storing data received while passing over one part of Earth and transmitting it later while passing over another part. This will be the case with the CASCADE system of Canada's CASSIOPE communications satellite. Another system using this store and forward method is Orbcomm.

## Medium Earth Orbit (MEO)

A MEO is a satellite in orbit somewhere between 2,000 and 35,786 kilometres (1,243 and 22,236 mi) above the earth's surface. MEO satellites are similar to LEO satellites in functionality. MEO satellites are visible for much longer periods of time than LEO satellites, usually between 2 and 8 hours. MEO satellites have a larger coverage area than LEO satellites. A MEO satellite's longer duration of visibility and wider footprint means fewer satellites are needed in a MEO network than a LEO network. One disadvantage is that a MEO satellite's distance gives it a longer time delay and weaker signal than a LEO satellite, although these limitations are not as severe as those of a GEO satellite.

Like LEOs, these satellites don't maintain a stationary distance from the earth. This is in contrast to the geostationary orbit, where satellites are always approximately 35,786 kilometres (22,236 mi) from the earth.

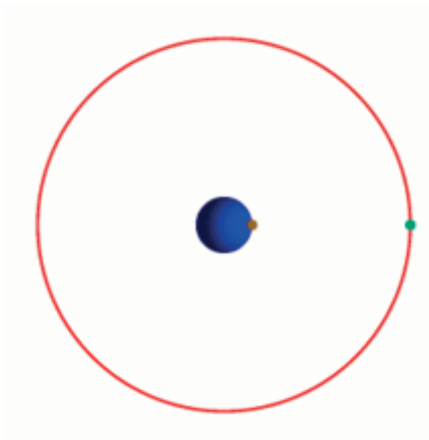
Typically the orbit of a medium earth orbit satellite is about 16,000 kilometres (10,000 mi) above earth. In various patterns, these satellites make the trip around earth in anywhere from 2–12 hours, which provides better coverage to wider areas than that provided by LEOs.

## Example

In 1962, the first communications satellite, Telstar, was launched. It was a medium earth orbit satellite designed to help facilitate high-speed telephone signals. Although it was

the first practical way to transmit signals over the horizon, its major drawback was soon realized. Because its orbital period of about 2.5 hours did not match the Earth's rotational period of 24 hours, continuous coverage was impossible. It was apparent that multiple MEOs needed to be used in order to provide continuous coverage.

## Geostationary Orbits (GEO)



Geostationary orbit

To an observer on the earth, a satellite in a geostationary orbit appears motionless, in a fixed position in the sky. This is because it revolves around the earth at the earth's own angular velocity (360 degrees every 24 hours, in an equatorial orbit).

A geostationary orbit is useful for communications because ground antennas can be aimed at the satellite without their having to track the satellite's motion. This is relatively inexpensive.

In applications that require a large number of ground antennas, such as DirecTV distribution, the savings in ground equipment can more than outweigh the cost and complexity of placing a satellite into orbit.

## Examples

- The first geostationary satellite was Syncom 3, launched on August 19, 1964, and used for communication across the Pacific starting with television coverage of the 1964 Summer Olympics. Shortly after Syncom 3, Intelsat I, aka *Early Bird*, was launched on April 6, 1965 and placed in orbit at 28° west longitude. It was the first geostationary satellite for telecommunications over the Atlantic Ocean.
- On November 9, 1972, Canada's first geostationary satellite serving the continent, Anik A1, was launched by Telesat Canada, with the United States following suit with the launch of Westar 1 by Western Union on April 13, 1974.

- On May 30, 1974, the first geostationary communications satellite in the world to be three-axis stabilized was launched: the experimental satellite ATS-6 built for NASA.
- After the launches of the Telstar through Westar 1 satellites, RCA Americom (later GE Americom, now SES) launched Satcom 1 in 1975. It was Satcom 1 that was instrumental in helping early cable TV channels such as WTBS (now TBS), HBO, CBN (now Freeform) and The Weather Channel become successful, because these channels distributed their programming to all of the local cable TV headends using the satellite. Additionally, it was the first satellite used by broadcast television networks in the United States, like ABC, NBC, and CBS, to distribute programming to their local affiliate stations. Satcom 1 was widely used because it had twice the communications capacity of the competing Westar 1 in America (24 transponders as opposed to the 12 of Westar 1), resulting in lower transponder-usage costs. Satellites in later decades tended to have even higher transponder numbers.

By 2000, Hughes Space and Communications (now Boeing Satellite Development Center) had built nearly 40 percent of the more than one hundred satellites in service worldwide. Other major satellite manufacturers include Space Systems/Loral, Orbital Sciences Corporation with the STAR Bus series, Indian Space Research Organisation, Lockheed Martin (owns the former RCA Astro Electronics/GE Astro Space business), Northrop Grumman, Alcatel Space, now Thales Alenia Space, with the Spacebus series, and Astrium.

## *Molniya Satellites*

Geostationary satellites must operate above the equator and therefore appear lower on the horizon as the receiver gets the farther from the equator. This will cause problems for extreme northerly latitudes, affecting connectivity and causing multipath interference (caused by signals reflecting off the ground and into the ground antenna).

Thus, for areas close to the North (and South) Pole, a geostationary satellite may appear below the horizon. Therefore, Molniya orbit satellites have been launched, mainly in Russia, to alleviate this problem.

Molniya orbits can be an appealing alternative in such cases. The Molniya orbit is highly inclined, guaranteeing good elevation over selected positions during the northern portion of the orbit. (Elevation is the extent of the satellite's position above the horizon. Thus, a satellite at the horizon has zero elevation and a satellite directly overhead has elevation of 90 degrees.)

The Molniya orbit is designed so that the satellite spends the great majority of its time over the far northern latitudes, during which its ground footprint moves only slightly. Its period is one half day, so that the satellite is available for operation over the targeted region for six to nine hours every second revolution. In this way a constellation of three Molniya satellites (plus in-orbit spares) can provide uninterrupted coverage.

The first satellite of the Molniya series was launched on April 23, 1965 and was used for experimental transmission of TV signals from a Moscow uplink station to downlink stations located in Siberia and the Russian Far East,

in Norilsk, Khabarovsk, Magadan and Vladivostok. In November 1967 Soviet engineers created a unique system of national TV network of satellite television, called Orbita, that was based on Molniya satellites.

### *Polar Orbit*

In the United States, the National Polar-orbiting Operational Environmental Satellite System (NPOESS) was established in 1994 to consolidate the polar satellite operations of NASA (National Aeronautics and Space Administration) NOAA (National Oceanic and Atmospheric Administration). NPOESS manages a number of satellites for various purposes; for example, METSAT for meteorological satellite, EUMETSAT for the European branch of the program, and METOP for meteorological operations.

These orbits are sun synchronous, meaning that they cross the equator at the same local time each day. For example, the satellites in the NPOESS (civilian) orbit will cross the equator, going from south to north, at times 1:30 P.M., 5:30 P.M., and 9:30 P.M.

## Structure

Communications Satellites are usually composed of the following subsystems:

- Communication Payload, normally composed of transponders, antennas, and switching systems
- Engines used to bring the satellite to its desired orbit
- Station Keeping Tracking and stabilization subsystem used to keep the satellite in the right orbit, with its antennas pointed in the right direction, and its power system pointed towards the sun
- Power subsystem, used to power the Satellite systems, normally composed of solar cells, and batteries that maintain power during solar eclipse
- Command and Control subsystem, which maintains communications with ground control stations. The ground control earth stations monitor the satellite performance and control its functionality during various phases of its life-cycle.

The bandwidth available from a satellite depends upon the number of transponders provided by the satellite. Each service (TV, Voice, Internet, radio) requires a different amount of bandwidth for transmission. This is typically known as link budgeting and a network simulator can be used to arrive at the exact value.

## Frequency Allocation for Satellite Systems

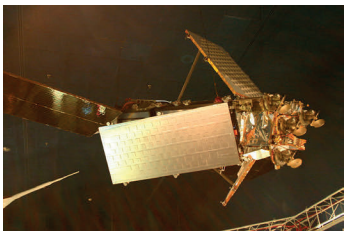
Allocating frequencies to satellite services is a complicated process which requires international coordination and planning. This is carried out under the auspices of the International Telecommunication Union (ITU). To facilitate frequency planning, the world is divided into three regions: Region 1: Europe, Africa, what was formerly the Soviet Union, and Mongolia Region 2: North and South America and Greenland Region 3: Asia (excluding region 1 areas), Australia, and the southwest Pacific

Within these regions, frequency bands are allocated to various satellite services, although a given service may be allocated different frequency bands in different regions. Some of the services provided by satellites are:

- Fixed satellite service (FSS)
- Broadcasting satellite service (BSS)
- Mobile satellite service
- Radionavigation-satellite service
- Meteorological-satellite service
- Amateur-satellite service

## Applications

### *Telephone*



An Iridium satellite

The first and historically most important application for communication satellites was in intercontinental long distance telephony. The fixed Public Switched Telephone Network relays telephone calls from land line telephones to an earth station, where they are then transmitted to a geostationary satellite. The downlink follows an analogous path. Improvements in submarine communications cables through the use of fiber-optics caused some decline in the use of satellites for fixed telephony in the late 20th century.

Satellite communications are still used in many applications today. Remote islands such as Ascension Island, Saint Helena, Diego Garcia, and Easter Island, where no submarine cables are in service, need satellite telephones. There are also regions of some continents and countries where landline telecommunications are rare to nonexistent, for example large regions of South America, Africa, Canada, China, Russia, and Australia. Satellite communications also provide connection to the edges of Antarctica and Greenland. Other land use for satellite phones are rigs at sea, a back up for hospitals, military, and recreation. Ships at sea, as well as planes, often use satellite phones.

Satellite phone systems can be accomplished by a number of means. On a large scale, often there will be a local telephone system in an isolated area with a link to the telephone system in a main land area. There are also services that will patch a radio signal to a telephone system. In this example, almost any type of satellite can be

used. Satellite phones connect directly to a constellation of either geostationary or low-earth-orbit satellites. Calls are then forwarded to a satellite teleport connected to the Public Switched Telephone Network.

## Television

As television became the main market, its demand for simultaneous delivery of relatively few signals of large bandwidth to many receivers being a more precise match for the capabilities of geosynchronous comsats. Two satellite types are used for North American television and radio: Direct broadcast satellite (DBS), and Fixed Service Satellite (FSS).

The definitions of FSS and DBS satellites outside of North America, especially in Europe, are a bit more ambiguous. Most satellites used for direct-to-home television in Europe have the same high power output as DBS-class satellites in North America, but use the same linear polarization as FSS-class satellites. Examples of these are the Astra, Eutelsat, and Hotbird spacecraft in orbit over the European continent. Because of this, the terms FSS and DBS are more so used throughout the North American continent, and are uncommon in Europe.

Fixed Service Satellites use the C band, and the lower portions of the $K_u$ band. They are normally used for broadcast feeds to and from television networks and local affiliate stations (such as program feeds for network and syndicated programming, live shots, and backhauls), as well as being used for distance learning by schools and universities, business television (BTV), Videoconferencing, and general commercial telecommunications. FSS satellites are also used to distribute national cable channels to cable television headends.

Free-to-air satellite TV channels are also usually distributed on FSS satellites in the $K_u$ band. The Intelsat Americas 5, Galaxy 10R and AMC 3 satellites over North America provide a quite large amount of FTA channels on their $K_u$ band transponders.

The American Dish Network DBS service has also recently utilized FSS technology as well for their programming packages requiring their SuperDish antenna, due to Dish Network needing more capacity to carry local television stations per the FCC's "must-carry" regulations, and for more bandwidth to carry HDTV channels.

A direct broadcast satellite is a communications satellite that transmits to small DBS satellite dishes (usually 18 to 24 inches or 45 to 60 cm in diameter). Direct broadcast satellites generally operate in the upper portion of the microwave $K_u$ band. DBS technology is used for DTH-oriented (Direct-To-Home) satellite TV services, such as DirecTV and DISH Network in the United States, Bell TV and Shaw Direct in Canada, Freesat and Sky in the UK, Ireland, and New Zealand and DSTV in South Africa.

Operating at lower frequency and lower power than DBS, FSS satellites require a much larger dish for reception (3 to 8 feet (1 to 2.5 m) in diameter for $K_u$ band, and 12 feet (3.6 m) or larger for C band). They use linear polarization for each of the transponders' RF input and output (as opposed to circular polarization used by DBS satellites), but this is a minor technical difference that users do not notice. FSS satellite technology was also originally used for DTH satellite TV from the late 1970s to the early 1990s in the

United States in the form of TVRO (TeleVision Receive Only) receivers and dishes. It was also used in its $K_u$ band form for the now-defunct Primestar satellite TV service.

Some satellites have been launched that have transponders in the $K_a$ band, such as DirecTV's SPACEWAY-1 satellite, and Anik F2. NASA and ISRO have also launched experimental satellites carrying $K_a$ band beacons recently.

Some manufacturers have also introduced special antennas for mobile reception of DBS television. Using Global Positioning System (GPS) technology as a reference, these antennas automatically re-aim to the satellite no matter where or how the vehicle (on which the antenna is mounted) is situated. These mobile satellite antennas are popular with some recreational vehicle owners. Such mobile DBS antennas are also used by JetBlue Airways for DirecTV (supplied by LiveTV, a subsidiary of JetBlue), which passengers can view on-board on LCD screens mounted in the seats.

## *Radio Broadcasting*

Satellite radio offers audio broadcast services in some countries, notably the United States. Mobile services allow listeners to roam a continent, listening to the same audio programming anywhere.

A satellite radio or subscription radio (SR) is a digital radio signal that is broadcast by a communications satellite, which covers a much wider geographical range than terrestrial radio signals.

Satellite radio offers a meaningful alternative to ground-based radio services in some countries, notably the United States. Mobile services, such as SiriusXM, and Worldspace, allow listeners to roam across an entire continent, listening to the same audio programming anywhere they go. Other services, such as Music Choice or Muzak's satellite-delivered content, require a fixed-location receiver and a dish antenna. In all cases, the antenna must have a clear view to the satellites. In areas where tall buildings, bridges, or even parking garages obscure the signal, repeaters can be placed to make the signal available to listeners.

Initially available for broadcast to stationary TV receivers, by 2004 popular mobile direct broadcast applications made their appearance with the arrival of two satellite radio systems in the United States: Sirius and XM Satellite Radio Holdings. Later they merged to become the conglomerate SiriusXM.

Radio services are usually provided by commercial ventures and are subscription-based. The various services are proprietary signals, requiring specialized hardware for decoding and playback. Providers usually carry a variety of news, weather, sports, and music channels, with the music channels generally being commercial-free.

In areas with a relatively high population density, it is easier and less expensive to reach the bulk of the population with terrestrial broadcasts. Thus in the UK and some other countries, the contemporary evolution of radio services is focused on Digital Audio Broadcasting (DAB) services or HD Radio, rather than satellite radio.

### Amateur Radio

Amateur radio operators have access to amateur satellites, which have been designed specifically to carry amateur radio traffic. Most such satellites operate as spaceborne repeaters, and are generally accessed by amateurs equipped with UHF or VHF radio equipment and highly directional antennas such as Yagis or dish antennas. Due to launch costs, most current amateur satellites are launched into fairly low Earth orbits, and are designed to deal with only a limited number of brief contacts at any given time. Some satellites also provide data-forwarding services using the X.25 or similar protocols.

### Internet Access

After the 1990s, satellite communication technology has been used as a means to connect to the Internet via broadband data connections. This can be very useful for users who are located in remote areas, and cannot access a broadband connection, or require high availability of services.

### Military

Communications satellites are used for military communications applications, such as Global Command and Control Systems. Examples of military systems that use communication satellites are the MILSTAR, the DSCS, and the FLTSATCOM of the United States, NATO satellites, United Kingdom satellites (for instance Skynet), and satellites of the former Soviet Union. India has launched its first Military Communication satellite GSAT-7, its transponders operate in UHF, F, C and $K_u$ band bands. Typically military satellites operate in the UHF, SHF (also known as X-band) or EHF (also known as $K_a$ band) frequency bands.

## MODEM

A modem (modulator-demodulator) is a network hardware device that modulates one or more carrier wave signals to encode digital information for transmission and demodulates signals to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used with any means of transmitting analog signals, from light emitting diodes to radio. A common type of modem is one that turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Modems are generally classified by the amount of data they can send in a given unit of time, usually expressed in bits per second (symbol bit/s, sometimes abbreviated "bps"), or bytes per second (symbol B/s). Modems can also be classified by their symbol rate, measured in baud. The baud unit denotes symbols per second, or the number of times per second the modem sends a new signal. For example, the ITU V.21 standard used audio frequency shift keying with two possible frequencies, corresponding to two distinct symbols (or one bit per symbol), to carry 300 bits per second using 300 baud. By contrast, the original ITU V.22 standard, which could transmit and receive four distinct

symbols (two bits per symbol), transmitted 1,200 bits by sending 600 symbols per second (600 baud) using phase shift keying.




Acoustic coupler modem

## Dialup Modem



TeleGuide terminal

News wire services in the 1920s used multiplex devices that satisfied the definition of a modem. However, the modem function was incidental to the multiplexing function, so they are not commonly included in the history of modems. Modems grew out of the need to connect teleprinters over ordinary phone lines instead of the more expensive leased lines which had previously been used for current loop–based teleprinters and automated telegraphs.

Mass-produced modems in the United States began as part of the SAGE air-defense system in 1958 (the year the word *modem* was first used), connecting terminals at various airbases, radar sites, and command-and-control centers to the SAGE director centers scattered around the U.S. and Canada. SAGE modems were described by AT&T's Bell Labs as conforming to their newly published Bell 101 dataset standard. While they ran on dedicated telephone lines, the devices at each end were no different from commercial acoustically coupled Bell 101, 110 baud modems.

The *201A* and *201B Data-Phones* were synchronous modems using two-bit-per-baud phase-shift keying (PSK). The 201A operated half-duplex at 2,000 bit/s over normal phone lines, while the 201B provided full duplex 2,400 bit/s service on four-wire leased lines, the send and receive channels each running on their own set of two wires.

The famous *Bell 103A dataset* standard was also introduced by AT&T in 1962. It provided full-duplex service at 300 bit/s over normal phone lines. Frequency-shift keying was used, with the call originator transmitting at 1,070 or 1,270 Hz and the answering modem transmitting at 2,025 or 2,225 Hz. The readily available 103A2 gave an important boost to the use of remote low-speed terminals such as the Teletype Model 33 ASR and KSR, and the IBM 2741. AT&T reduced modem costs by introducing the originate-only 113D and the answer-only 113B/C modems.

## Acoustic Couplers




The *Novation CAT* acoustically coupled modem

For many years, the Bell System (AT&T) maintained a monopoly on the use of its phone lines and what devices could be connected to them. However, the seminal *Hush-a-Phone v. FCC* case of 1956 concluded it was within the FCC's jurisdiction to regulate the operation of the Bell System. The FCC found that as long as a device was not electronically attached to the system, it would not threaten its integrity. This led to a number of devices that *mechanically* connected to the phone through a standard handset. Since most handsets were supplied by Western Electric and thus of a standard design, acoustic couplers were relatively easy to build. This type of connection was used for many devices, such as answering machines.

Acoustically coupled Bell 103A-compatible 300 bit/s modems were common during the 1970s. Well-known models included the Novation CAT and the Anderson-Jacobson, the latter spun off from an in-house project at Stanford Research Institute (now SRI International). An even lower-cost option was the Pennywhistle modem, designed to be built using parts from electronics scrap and surplus stores.

In December 1972, Vadic introduced the *VA3400*, notable for full-duplex operation at 1,200 bit/s over the phone network. Like the 103A, it used different frequency bands for transmit and receive. In November 1976, AT&T introduced the 212A modem to compete with Vadic. It was similar in design, but used the lower frequency set for transmission. One could also use the 212A with a 103A modem at 300 bit/s. According to Vadic, the change in frequency assignments made the 212 intentionally incompatible with acoustic coupling, thereby locking out many potential modem manufacturers. In 1977, Vadic responded with the VA3467 triple modem, an answer-only modem sold to computer center operators that supported Vadic's 1,200-bit/s mode, AT&T's 212A mode, and 103A operation.

## Carterfone and Direct Connection

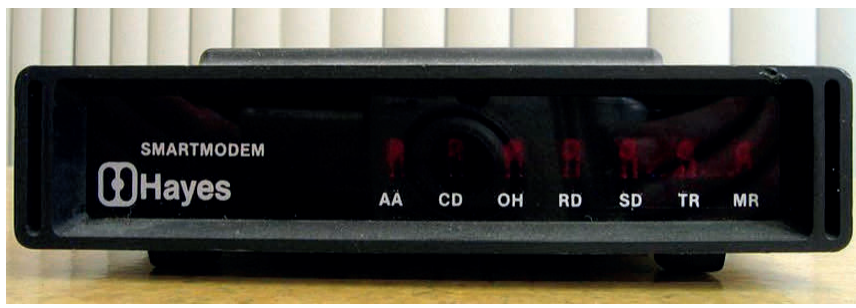
The *Hush-a-Phone* decision applied only to mechanical connections, but the *Carterfone* decision of 1968, led to the FCC introducing a rule setting stringent AT&T-designed tests for electronically coupling a device to the phone lines. This opened the door to direct-connect modems that plugged directly into the phone line rather than via a handset. However, the cost of passing the tests was considerable, and acoustically coupled modems remained common into the early 1980s.

The rapidly falling prices of electronics in the late 1970s led to an increasing number of direct-connect models around 1980. In spite of being directly connected, these modems were generally operated like their earlier acoustic versions – dialling and other phone-control operations were completed by hand, using an attached handset. A small number of modems added the ability to automatically answer incoming calls, or automatically place an outgoing call to a single number, but even these limited features were relatively rare or limited to special models in a lineup. When more flexible solutions were needed, 3rd party "dialers" were used to automate calling, normally using a separate serial port to communicate with the dialler, which would then control the modem through a private electrical connection.

The introduction of microcomputer systems with internal expansion slots made the first software-controllable modems common. Slot connections gave the computer

complete access to the modem's memory or I/O channels, which allowed software to send commands to the modem, not just data. This led to a series of popular modems for the S-100 bus and Apple II computers that could directly dial the phone, answer incoming calls, and hang up the phone, the basic requirements of a bulletin board system (BBS). The seminal CBBS was created on an S-100 machine with a Hayes internal modem, and a number of similar systems followed.

## The Smartmodem and the Rise of BBSs




The original model 300-baud Smartmodem

The next major advance in modems was the *Hayes Smartmodem*, introduced in 1981. The Smartmodem was an otherwise standard 103A 300-bit/s direct-connect modem, but it was attached to a small microcontroller that watched the data stream for certain character strings representing commands. This allowed both data and commands to be sent through a single serial port. The now-standard Hayes command set included instructions for picking up and hanging up the phone, dialing numbers, and answering calls, among others. This was similar to the commands offered by the internal modems, but unlike them, the Smartmodem could be connected to any computer with an RS-232 port, which was practically every microcomputer built.

The introduction of the Smartmodem made communications much simpler and more easily accessed. This provided a growing market for other vendors, who licensed the Hayes patents and competed on price or by adding features. Through the 1980s, a number of new higher-speed modems, first 1,200 and then 2,400 bit/s, greatly improved the responsiveness of the online systems, and made file transfer practical. This led to rapid growth of online services with their large file libraries, which in turn gave more reason to own a modem. The rapid update of modems led to a similar rapid increase in BBS use, which was helped by the fact that BBSs could control the modem simply by sending strings, rather than talking to a device driver that was different for every direct-connect modem.

## 1200 and 2400 bit/s

The 300 bit/s modems used audio frequency-shift keying to send data. In this system the stream of 1s and 0s in computer data is translated into sounds which can be easily sent

on the phone lines. In the Bell 103 system, the originating modem sends 0s by playing a 1,070 Hz tone, and 1s at 1,270 Hz, with the *answering* modem transmitting its 0s on 2,025 Hz and 1s on 2,225 Hz. These frequencies were chosen carefully; they are in the range that suffers minimum distortion on the phone system and are not harmonics of each other.

In the 1,200 bit/s and faster systems, phase-shift keying was used. In this system the two tones for any one side of the connection are sent at similar frequencies as in the 300 bit/s systems, but slightly out of phase. Voiceband modems generally remained at 300 and 1,200 bit/s (V.21 and V.22) into the mid-1980s. A V.22bis 2,400-bit/s system similar in concept to the 1,200-bit/s Bell 212 signaling was introduced in the U.S., and a slightly different one in Europe. The limited available frequency range meant the symbol rate of 1,200 bit/s modems was still only 600 baud (symbols per second). The bit rate increases were achieved by defining four or eight distinct symbols, which allowed the encoding of two or three bits per symbol instead of only 1. The use of smaller shifts had the drawback of making each symbol more vulnerable to interference, but improvements in phone line quality at the same time helped compensate for this. By the late 1980s, most modems could support all of these standards and 2,400-bit/s operation was becoming common.

## Proprietary Standards

Many other standards were also introduced for special purposes, commonly using a high-speed channel for receiving, and a lower-speed channel for sending. One typical example was used in the French Minitel system, in which the user's terminals spent the majority of their time receiving information. The modem in the Minitel terminal thus operated at 1,200 bit/s for reception, and 75 bit/s for sending commands back to the servers.

Three U.S. companies became famous for high-speed versions of the same concept. Telebit introduced its *Trailblazer* modem in 1984, which used a large number of 36 bit/s channels to send data one-way at rates up to 18,432 bit/s. A single additional channel in the reverse direction allowed the two modems to communicate how much data was waiting at either end of the link, and the modems could change direction on the fly. The Trailblazer modems also supported a feature that allowed them to spoof the UUCP *g* protocol, commonly used on Unix systems to send e-mail, and thereby speed UUCP up by a tremendous amount. Trailblazers thus became extremely common on Unix systems, and maintained their dominance in this market well into the 1990s.

USRobotics (USR) introduced a similar system, known as *HST*, although this supplied only 9,600 bit/s (in early versions at least) and provided for a larger backchannel. Rather than offer spoofing, USR instead created a large market among Fidonet users by offering its modems to BBS sysops at a much lower price, resulting in sales to end users who wanted faster file transfers. Hayes was forced to compete, and introduced its own 9,600-bit/s standard, *Express 96* (also known as *Ping-Pong*), which was generally similar to Telebit's PEP. Hayes, however, offered neither protocol spoofing nor sysop discounts, and its high-speed modems remained rare.

A common feature of these high-speed modems was the concept of fallback, or *speed hunting*, allowing them to communicate with less-capable modems. During the call initiation, the modem would transmit a series of signals and wait for the remote modem

to respond. They would start at high speeds and get progressively slower until there was a response. Thus, two USR modems would be able to connect at 9,600 bit/s, but, when a user with a 2,400 bit/s modem called in, the USR would fall back to the common 2,400 bit/s speed. This would also happen if a V.32 modem and a HST modem were connected. Because they used a different standard at 9,600 bit/s, they would fall back to their highest commonly supported standard at 2,400 bit/s. The same applies to V.32bis and 14,400 bit/s HST modem, which would still be able to communicate with each other at 2,400 bit/s.

## *Echo cancellation, 9600 and 14,400*




USRobotics Sportster 14,400 Fax modem (1994)

Echo cancellation was the next major advance in modem design.

Local telephone lines use the same wires to send and receive data, which results in a small amount of the outgoing signal being reflected back. This is useful for people talking on the phone, as it provides a signal to the speaker that their voice is making it through the system. However, this reflected signal causes problems for the modem, which is unable to distinguish between a signal from the remote modem and the echo of its own signal. This was why earlier modems split the signal frequencies into "answer" and "originate"; the modem could then ignore any signals in the frequency range it was using for transmission. Even with improvements to the phone system allowing higher speeds, this splitting of available phone signal bandwidth still imposed a half-speed limit on modems.

Echo cancellation eliminated this problem. During the call setup and negotiation period, both modems send a series of unique tones and then listen for them to return through the phone system. They measure the total delay time and then set up a local delay loop to the same time. Once the connection is completed, they send their signals into the phone lines as normal, but also into the delay, which is inverted. The signal returning through the echo meets the inverted version coming from the delay line, and cancels out the echo. This allowed both modems to use the full spectrum available, doubling the speed.

Additional improvements were introduced via the Quadrature Amplitude Modulation (QAM) encoding system. Previous systems using phase shift keying (PSK) encoded two bits (or sometimes three) per symbol by slightly delaying or advancing the signal's phase relative to a set carrier tone. QAM used a combination of phase shift and amplitude to encode four bits per symbol. Transmitting at 1,200 baud produced the 4,800 bit/s V.27ter standard, the same working at a base rate of 2,400 baud produced the 9,600 bit/s V.32. The carrier frequency was 1,650 Hz in both systems. For many years, most engineers considered this rate to be the limit of data communications over telephone networks.

The introduction of these higher-speed systems also led to the digital fax machine during the 1980s. Digital faxes are simply an image format sent over a high-speed (commonly 14.4 kbit/s) modem. Software running on the host computer can convert any image into fax format, which can then be sent using the modem. Such software was at one time an add-on, but has since become largely universal.

## Breaking the 9.6 Kbit/s Barrier

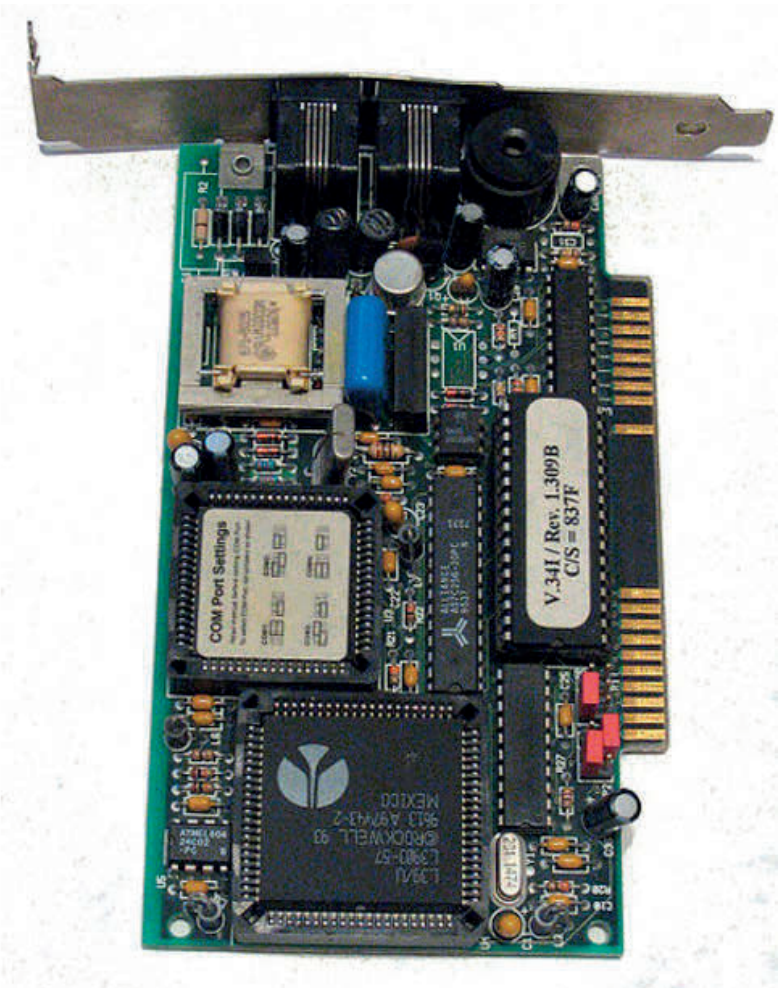
In 1980, Gottfried Ungerboeck from IBM Zurich Research Laboratory applied channel coding techniques to search for new ways to increase the speed of modems. His results were astonishing but only conveyed to a few colleagues. In 1982, he agreed to publish what is now a landmark paper in the theory of information coding. By applying parity check coding to the bits in each symbol, and mapping the encoded bits into a two-dimensional diamond pattern, Ungerboeck showed that it was possible to increase the speed by a factor of two with the same error rate. The new technique was called *mapping by set partitions*, now known as trellis modulation.

Error correcting codes, which encode code words (sets of bits) in such a way that they are far from each other, so that in case of error they are still closest to the original word (and not confused with another) can be thought of as analogous to sphere packing or packing pennies on a surface: the further two bit sequences are from one another, the easier it is to correct minor errors.

V.32 modems operating at 9600 bit/s were expensive and were only starting to enter the market in the early 1990s when V.32bis was standardized. Rockwell International's chip division developed a new driver chip set incorporating the standard and aggressively priced it. Supra, Inc. arranged a short-term exclusivity arrangement with Rockwell, and developed the SupraFAXmodem 14400 based on it. Introduced in January 1992 at $399 (or less), it was half the price of the slower V.32 modems already on the market. This led to a price war, and by the end of the year V.32 was dead, never having been really established, and V.32bis modems were widely available for $250.

V.32bis was so successful that the older high-speed standards had little to recommend them. USR fought back with a 16,800 bit/s version of HST, while AT&T introduced a one-off 19,200 bit/s method they referred to as V.32ter, but neither non-standard modem sold well.

## V.34/28.8 Kbit/s and 33.6 Kbit/s




V.34 modem in the shape of an internal ISA card




V.34 data/fax modem as PC card for notebooks






External V.34 modem with RS-232 serial port

Any interest in these proprietary improvements was destroyed during the lengthy introduction of the 28,800 bit/s V.34 standard. While waiting, several companies decided to release hardware and introduced modems they referred to as *V.FAST*. In order to guarantee compatibility with V.34 modems once the standard was ratified (1994), the manufacturers were forced to use more flexible parts, generally a DSP and microcontroller, as opposed to purpose-designed ASIC modem chips.

The ITU standard V.34 represents the culmination of the joint efforts. It employs the most powerful coding techniques including channel encoding and shape encoding. From the mere four bits per symbol (9.6 kbit/s), the new standards used the functional equivalent of 6 to 10 bits per symbol, plus increasing baud rates from 2,400 to 3,429, to create 14.4, 28.8, and 33.6 kbit/s modems. This rate is near the theoretical Shannon limit. When calculated, the Shannon capacity of a narrowband line is $\text{bandwidth} \times \log_2(1 + P_u/P_n)$, with $P_u/P_n$ the (linear) signal-to-noise ratio. Narrowband phone lines have a bandwidth of 3,000 Hz so using $P_u/P_n = 1000$ (SNR = 30 dB), the capacity is approximately 30 kbit/s.

Without the discovery and eventual application of trellis modulation, maximum telephone rates using voice-bandwidth channels would have been limited to 3,429 baud × 4 bit/symbol = approximately 14 kbit/s using traditional QAM.

## Using Digital Lines and PCM (V.90/92)



Modem bank at an ISP

During the late 1990s, Rockwell-Lucent and USRobotics introduced competing technologies based upon the digital transmission used in telephony networks. The standard digital transmission in modern networks is 64 kbit/s but some networks use a part of the bandwidth for remote office signaling (e.g. to hang up the phone), limiting the effective rate to 56 kbit/s DS0. This new technology was adopted into ITU standards V.90 and is common in modern computers. The 56 kbit/s rate is only possible from the central office to the user site (downlink). In the United States, government regulation limits the maximum power output, resulting in a maximum data rate of 53.3 kbit/s. The uplink (from the user to the central office) still uses V.34 technology at 33.6 kbit/s. USRobotics began work on the technology first, calling theirs X2 because 56k was twice the speed of 28k modems. USRobotics held a 40-percent share of the retail modem market, and Rockwell International held an 80-percent share of the modem chipset market. Concerned with being shut out of the market, Rockwell began work on a rival 56k technology and joined with Lucent and Motorola on what it called K56Flex or Flex. Both technologies reached the market around February 1997; although problems with K56Flex modems were noted in product reviews through July, within six months they worked equally well with variations dependent on local connection characteristics. The retail price of the 56K modems was about US$200, compared to $100 for 33K modems. Separate equipment was required by Internet service providers (ISPs) to support the incompatible technologies, with costs varying depending on whether their current equipment could be upgraded. About half of all ISPs offered 56K support by October 1997. Consumer sales were relatively low, which USRobotics and Rockwell attributed to conflicting standards.

The International Telecommunication Union (ITU) announced the draft of a new 56 kbit/s standard, V.90, in February 1998, with strong industry support. Incompatible with either existing standard, it was an amalgam of both which was designed to allow both types of modem to be converted to it by a firmware upgrade. This V.90 standard was approved in September 1998, and widely adopted by ISPs and consumers.

Later in V.92, the digital PCM technique was applied to increase the upload speed to a maximum of 48 kbit/s, but at the expense of download rates. A 48 kbit/s upstream rate would reduce the downstream as low as 40 kbit/s due to echo on the telephone line. To avoid this problem, V.92 modems offer the option to turn off the digital upstream and instead use a 33.6 kbit/s analog connection, in order to maintain a high digital downstream of 50 kbit/s or higher. V.92 also adds two other features. The first is the ability for users who have call waiting to put their dial-up Internet connection on hold for extended periods of time while they answer a call. The second feature is the ability to quickly connect to one's ISP. This is achieved by remembering the analog and digital characteristics of the telephone line, and using this saved information when reconnecting.

## *Using Compression to Exceed 56 Kbit/S*

V.42, V.42bis and V.44 standards allow the modem to transmit data faster than its basic rate would imply. For instance, a 53.3 kbit/s connection with V.44 can transmit up to $53.3 \times 6 = 320$ kbit/s using pure text. However, the compression ratio tends to vary due to noise on the line, or due to the transfer of already-compressed files (ZIP files, JPEG images, MP3 audio, MPEG video). At some points the modem will be sending

compressed files at approximately 50 kbit/s, uncompressed files at 160 kbit/s, and pure text at 320 kbit/s, or any value in between.

In such situations a small amount of memory in the modem, a buffer, is used to hold the data while it is being compressed and sent across the phone line, but in order to prevent overflow of the buffer, it sometimes becomes necessary to tell the computer to pause the datastream. This is accomplished through *hardware flow control* using extra lines on the modem–computer connection. The computer is then set to supply the modem at some higher rate, such as 320 kbit/s, and the modem will tell the computer when to start or stop sending data.

## Radio

Direct broadcast satellite, WiFi, and mobile phones all use modems to communicate, as do most other wireless services today. Modern telecommunications and data networks also make extensive use of radio modems where long distance data links are required. Such systems are an important part of the PSTN, and are also in common use for high-speed computer network links to outlying areas where fibre is not economical.

Even where a cable is installed, it is often possible to get better performance or make other parts of the system simpler by using radio frequencies and modulation techniques through a cable. Coaxial cable has a very large bandwidth, but signal attenuation becomes a major problem at high data rates if a baseband digital signal is used. By using a modem, a much larger amount of digital data can be transmitted through a single wire. Digital cable television and cable Internet services use radio frequency modems to provide the increasing bandwidth needs of modern households. Using a modem also allows for frequency-division multiple access to be used, making full-duplex digital communication with many users possible using a single wire.

Wireless modems come in a variety of types, bandwidths, and speeds. Wireless modems are often referred to as transparent or smart. They transmit information that is modulated onto a carrier frequency to allow many simultaneous wireless communication links to work simultaneously on different frequencies.

Transparent modems operate in a manner similar to their phone line modem cousins. Typically, they were half duplex, meaning that they could not send and receive data at the same time. Typically transparent modems are polled in a round robin manner to collect small amounts of data from scattered locations that do not have easy access to wired infrastructure. Transparent modems are most commonly used by utility companies for data collection.

Smart modems come with media access controllers inside, which prevents random data from colliding and resends data that is not correctly received. Smart modems typically require more bandwidth than transparent modems, and typically achieve higher data rates. The IEEE 802.11 standard defines a short range modulation scheme that is used on a large scale throughout the world.

## WiFi and WiMax

The WiFi and WiMax standards use wireless mobile broadband modems operating at microwave frequencies.

## Mobile Broadband




Huawei HSPA+ Evolution-Data Optimized (EVDO) USB wireless modem from Movistar Colombia

Modems which use a mobile telephone system (GPRS, UMTS, HSPA, EVDO, WiMax, etc.), are known as mobile broadband modems (sometimes also called wireless modems). Wireless modems can be embedded inside a laptop or appliance, or be external to it. External wireless modems are connect cards, USB modems for mobile broadband and cellular routers. A connect card is a PC Card or ExpressCard which slides into a PCMCIA/PC card/ExpressCard slot on a computer. USB wireless modems use a USB port on the laptop instead of a PC card or ExpressCard slot. A USB modem used for mobile broadband Internet is also sometimes referred to as a dongle. A cellular router may have an external datacard (*AirCard*) that slides into it. Most cellular routers do allow such datacards or USB modems. Cellular routers may not be modems by definition, but they contain modems or allow modems to be slid into them. The difference between a cellular router and a wireless modem is that a cellular router normally allows multiple people to connect to it (since it can route data or support multi-point to multi-point connections), while a modem is designed for one connection.

Most of GSM wireless modems come with an integrated SIM cardholder (i.e., Huawei E220, Sierra 881, etc.) and some models are also provided with a microSD memory slot and/or jack for additional external antenna such as Huawei E1762 and Sierra Wireless

Compass 885. The CDMA (EVDO) versions do not use R-UIM cards, but use Electronic Serial Number (ESN) instead.

The cost of using a wireless modem varies from country to country. Some carriers implement flat rate plans for unlimited data transfers. Some have caps (or maximum limits) on the amount of data that can be transferred per month. Other countries have plans that charge a fixed rate per data transferred—per megabyte or even kilobyte of data downloaded; this tends to add up quickly in today's content-filled world, which is why many people are pushing for flat data rates.

The faster data rates of the newest wireless modem technologies (UMTS, HSPA, EVDO, WiMax) are also considered to be *broadband wireless modems* and compete with other broadband modems below.

Until the end of April 2011, worldwide shipments of USB modems surpassed embedded 3G and 4G modules by 3:1 because USB modems can be easily discarded, but embedded modems could start to gain popularity as tablet sales grow and as the incremental cost of the modems shrinks, so by 2016, the ratio may change to 1:1.

Like mobile phones, mobile broadband modems can be SIM locked to a particular network provider. Unlocking a modem is achieved the same way as unlocking a phone, by using an ‹unlock code'.

## Residential Gateways

Some devices referred to as "broadband modems" are residential gateways, integrating the functions of a modem, network address translation (NAT) router, Ethernet switch, WiFi access point, DHCP server, firewall, among others. Some residential gateway offer a so-called "bridged mode", which disables the built-in routing function and makes the device function similarly to a plain modem. This bridged mode is separate from RFC 1483 bridging.

## Optical Modems

Fiber optic systems can be upgraded by the use of Quadrature amplitude modulation. The modulator and demodulator are separate components rather than a single assembly as with most modems.

## QAM16

16QAM uses a 16-point constellation to send four bits per baud. Speeds are usually on the order of 200 or 400 gigabit/sec.

## QAM64

64QAM uses a 64-point constellation to send six bits per baud. Although suppliers have announced components, announcements of installation are rare. Speeds of 65 Terabit-per-second have been observed.

### Home Networking

Although the name *modem* is seldom used in this case, modems are also used for high-speed home networking applications, especially those using existing home wiring. One example is the G.hn standard, developed by ITU-T, which provides a high-speed (up to 1 Gbit/s) Local area network using existing home wiring (power lines, phone lines and coaxial cables). G.hn devices use orthogonal frequency-division multiplexing (OFDM) to modulate a digital signal for transmission over the wire.

The phrase "null modem" was used to describe attaching a specially wired cable between the serial ports of two personal computers. Basically, the transmit output of one computer was wired to the receive input of the other; this was true for both computers. The same software used with modems (such as Procomm or Minicom) could be used with the null modem connection.

### Voice Modem

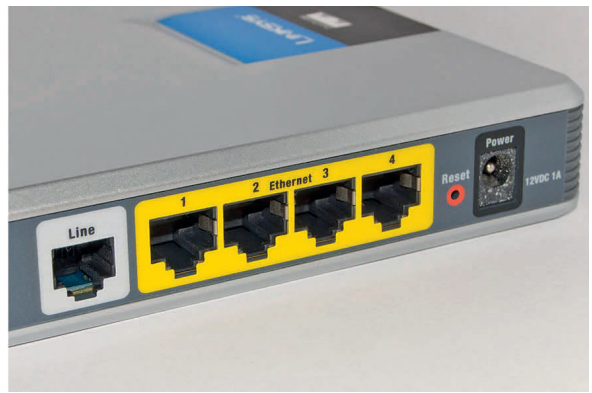
Voice modems are regular modems that are capable of recording or playing audio over the telephone line. They are used for telephony applications. See Voice modem command set for more details on voice modems. This type of modem can be used as an FXO card for Private branch exchange systems (compare V.92).

## ROUTER (COMPUTING)

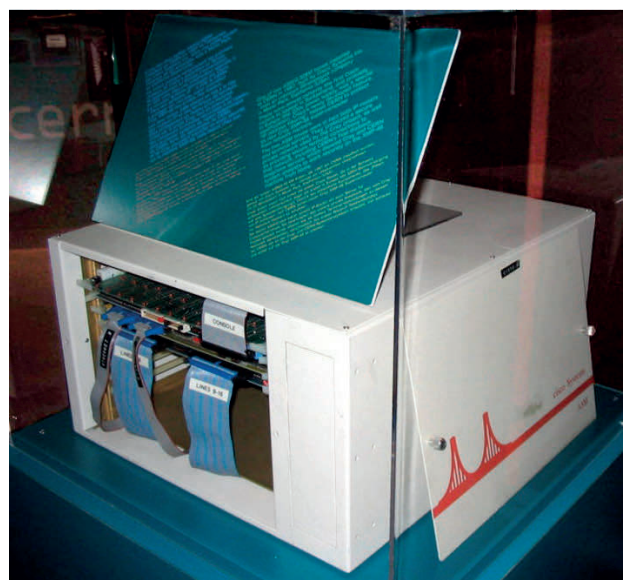
A **router** is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

A router is connected to two or more data lines from different networks.[b] When a data packet comes in on one of the lines, the router reads the address information in the packet to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. This creates an overlay internetwork.

The most familiar type of routers are home and small office routers that simply pass IP packets between the home computers and the Internet. An example of a router would be the owner's cable or DSL router, which connects to the Internet through an Internet service provider (ISP). More sophisticated routers, such as enterprise routers, connect large business or ISP networks up to the powerful core routers that forward data at high speed along the optical fiber lines of the Internet backbone. Though routers are typically dedicated hardware devices, software-based routers also exist.




A typical home or small office router showing the ADSL telephone line and Ethernet network cable connections



A Cisco ASM/2-32EM router deployed at CERN in 1987

## Applications

When multiple routers are used in interconnected networks, the routers can exchange information about destination addresses using a dynamic routing protocol. Each router builds up a routing table listing the preferred routes between any two systems on the interconnected networks.

A router may have interfaces for different physical types of network connections, such as copper cables, fibre optic, or wireless transmission. Its firmware can also support different networking communications protocol standards. Each network interface is used

by this specialized computer software to enable data packets to be forwarded from one protocol transmission system to another.

Routers may also be used to connect two or more logical groups of computer devices known as subnets, each with a different network prefix. The network prefixes recorded in the routing table do not necessarily map directly to the physical interface connections.

A router has two stages of operation called planes:

- Control plane: A router maintains a routing table that lists which route should be used to forward a data packet, and through which physical interface connection. It does this using internal pre-configured directives, called static routes, or by learning routes using a dynamic routing protocol. Static and dynamic routes are stored in the Routing Information Base (RIB). The control-plane logic then strips non-essential directives from the RIB and builds a Forwarding Information Base (FIB) to be used by the forwarding-plane.
- Forwarding plane: The router forwards data packets between incoming and outgoing interface connections. It routes them to the correct network type using information that the packet header contains. It uses data recorded in the routing table control plane.

Routers may provide connectivity within enterprises, between enterprises and the Internet, or between internet service providers' (ISPs) networks. The largest routers (such as the Cisco CRS-1 or Juniper T1600) interconnect the various ISPs, or may be used in large enterprise networks.Smaller routers usually provide connectivity for typical home and office networks. Other networking solutions may be provided by a backbone Wireless Distribution System (WDS), which avoids the costs of introducing networking cables into buildings.

All sizes of routers may be found inside enterprises. The most powerful routers are usually found in ISPs, academic and research facilities. Large businesses may also need more powerful routers to cope with ever increasing demands of intranet data traffic. A three-layer model is in common use, not all of which need be present in smaller networks.

## Access




A screenshot of the LuCI web interface used by OpenWrt. This page configures Dynamic DNS.

Access routers, including 'small office/home office' (SOHO) models, are located at customer sites such as branch offices that do not need hierarchical routing of their own. Typically, they are optimized for low cost. Some SOHO routers are capable of running alternative free Linux-based firmwares like Tomato, OpenWrt or DD-WRT.

### 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 are often responsible for enforcing quality of service across a wide area network (WAN), so they may have considerable memory installed, multiple WAN interface connections, and substantial onboard data processing routines. They may also provide connectivity to groups of file servers or other external networks.

### Security

External networks must be carefully considered as part of the overall security strategy. A router may include a firewall, VPN handling, and other security functions, or these may be handled by separate devices. Many companies produced security-oriented routers, including Cisco PIX series, Juniper NetScreen and WatchGuard. Routers also commonly perform network address translation, (which allows multiple devices on a network to share a single public IP address) and stateful packet inspection. Some experts argue that open source routers are more secure and reliable than closed source routers because open source routers allow mistakes to be quickly found and corrected.

### Core

In enterprises, a core router may provide a "collapsed backbone" interconnecting the distribution tier routers from multiple buildings of a campus, or large enterprise locations. They tend to be optimized for high bandwidth, but lack some of the features of edge routers.

### Internet Connectivity and Internal Use

Routers intended for ISP and major enterprise connectivity usually exchange routing information using the Border Gateway Protocol (BGP). RFC 4098 standard defines the types of BGP routers according to their functions:

- *Edge router*: Also called a provider edge router, is placed at the edge of an ISP network. The router uses External BGP to EBGP routers in other ISPs, or a large enterprise Autonomous System.
- *Subscriber edge router*: Also called a Customer Edge router, is located at the edge of the subscriber's network, it also uses EBGP to its provider's Autonomous System. It is typically used in an (enterprise) organization.
- *Inter-provider border router*: Interconnecting ISPs, is a BGP router that maintains BGP sessions with other BGP routers in ISP Autonomous Systems.

- Core router: A *core router* resides within an Autonomous System as a back bone to carry traffic between edge routers.
- Within an ISP: In the ISP's Autonomous System, a router uses internal BGP to communicate with other ISP edge routers, other intranet core routers, or the ISP's intranet provider border routers.
- "Internet backbone:" The Internet no longer has a clearly identifiable backbone, unlike its predecessor networks. See default-free zone (DFZ). The major ISPs' system routers make up what could be considered to be the current Internet backbone core. ISPs operate all four types of the BGP routers described here. An ISP "core" router is 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 protocols.
- Port forwarding: Routers are also used for port forwarding between private Internet-connected servers.
- Voice/Data/Fax/Video Processing Routers: Commonly referred to as access servers or gateways, these devices are used to route and process voice, data, video and fax traffic on the Internet. Since 2005, most long-distance phone calls have been processed as IP traffic (VOIP) through a voice gateway. Use of access server type routers expanded with the advent of the Internet, first with dial-up access and another resurgence with voice phone service.
- Larger networks commonly use multilayer switches, with layer 3 devices being used to simply interconnect multiple subnets within the same security zone, and higher layer switches when filtering, translation, load balancing or other higher level functions are required, especially between zones.

## Historical and Technical Information



Avaya ERS 8600 (2010)

The very first device that had fundamentally the same functionality as a router does today was the Interface Message Processor (IMP); IMPs were the devices that made up the ARPANET, the first TCP/IP network. The idea for a router (called "gateways" at the time) initially came about through an international group of computer networking researchers called the International Network Working Group (INWG). Set up in 1972 as an informal group to consider the technical issues involved in connecting different networks, later that year it became a subcommittee of the International Federation for Information Processing. These devices were different from most previous packet switching schemes in two ways. First, they connected dissimilar kinds of networks, such as serial lines and local area networks. Second, they were connectionless devices, which had no role in assuring that traffic was delivered reliably, leaving that entirely to the hosts.

The idea was explored in more detail, with the intention to produce a prototype system as part of two contemporaneous programs. One was the initial DARPA-initiated program, which created the TCP/IP architecture in use today. The other was a program at Xerox PARC to explore new networking technologies, which produced the PARC Universal Packet system; due to corporate intellectual property concerns it received little attention outside Xerox for years. Some time after early 1974, the first Xerox routers became operational. The first true IP router was developed by Virginia Strazisar at BBN, as part of that DARPA-initiated effort, during 1975-1976. By the end of 1976, three PDP-11-based routers were in service in the experimental prototype Internet.

The first multiprotocol routers were independently created by staff researchers at MIT and Stanford in 1981; the Stanford router was done by William Yeager, and the MIT one by Noel Chiappa; both were also based on PDP-11s. Virtually all networking now uses TCP/IP, but multiprotocol routers are still manufactured. They were important in the early stages of the growth of computer networking when protocols other than TCP/IP were in use. Modern Internet routers that handle both IPv4 and IPv6 are multiprotocol but are simpler devices than routers processing AppleTalk, DECnet, IP and Xerox protocols.

From the mid-1970s and in the 1980s, general-purpose mini-computers served as routers. Modern high-speed routers are highly specialized computers with extra hardware added to speed both common routing functions, such as packet forwarding, and specialised functions such as IPsec encryption. There is substantial use of Linux and Unix software based machines, running open source routing code, for research and other applications. Cisco's operating system was independently designed. Major router operating systems, such as those from Juniper Networks and Extreme Networks, are extensively modified versions of Unix software.

## Forwarding

The main purpose of a router is to connect multiple networks and forward packets destined either for its own networks or other networks. A router is considered a layer-3 device because its primary forwarding decision is based on the information in the layer-3 IP packet, specifically the destination IP address. When a router receives a packet, it searches its routing table to find the best match between the destination IP address of the packet and one of the addresses in the routing table. Once a match is found, the packet is encapsulated in the layer-2 data link frame for the outgoing interface indicated in the table entry. A

router typically does not look into the packet payload, but only at the layer-3 addresses to make a forwarding decision, plus optionally other information in the header for hints on, for example, quality of service (QoS). For pure IP forwarding, a router is designed to minimize the state information associated with individual packets. Once a packet is forwarded, the router does not retain any historical information about the packet.

The routing table itself can contain information derived from a variety of sources, such as a default or static routes that are configured manually, or dynamic routing protocols where the router learns routes from other routers. A default route is one that is used to route all traffic whose destination does not otherwise appear in the routing table; this is common – even necessary – in small networks, such as a home or small business where the default route simply sends all non-local traffic to the Internet service provider. The default route can be manually configured (as a static route), or learned by dynamic routing protocols, or be obtained by DHCP.

A router can run more than one routing protocol at a time, particularly if it serves as an autonomous system border router between parts of a network that run different routing protocols; if it does so, then redistribution may be used (usually selectively) to share information between the different protocols running on the same router.

Besides making a decision as to which interface a packet is forwarded to, which is handled primarily via the routing table, a router also has to manage congestion when packets arrive at a rate higher than the router can process. Three policies commonly used in the Internet are tail drop, random early detection (RED), and weighted random early detection (WRED). Tail drop is the simplest and most easily implemented; the router simply drops new incoming packets once the length of the queue exceeds the size of the buffers in the router. RED probabilistically drops datagrams early when the queue exceeds a pre-configured portion of the buffer, until a pre-determined max, when it becomes tail drop. WRED requires a weight on the average queue size to act upon when the traffic is about to exceed the pre-configured size, so that short bursts will not trigger random drops.

Another function a router performs is to decide which packet should be processed first when multiple queues exist. This is managed through QoS, which is critical when Voice over IP is deployed, so as not to introduce excessive latency.

Yet another function a router performs is called policy-based routing where special rules are constructed to override the rules derived from the routing table when a packet forwarding decision is made.

Router functions may be performed through the same internal paths that the packets travel inside the router. Some of the functions may be performed through an application-specific integrated circuit (ASIC) to avoid overhead of scheduling CPU time to process the packets. Others may have to be performed through the CPU as these packets need special attention that cannot be handled by an ASIC.

## REFERENCES

1. “Telecoms equipment - We have the technology”. The Economist. 1 October 1998. Retrieved 21 July 2012.
2. “Twisted pair - Nokia and Siemens pool their network divisions to form a new

firm". The Economist. 22 June 2006. Retrieved 21 July 2012.

3. Ypsilanti, Dimitri; Plantin, Amy (1991). Telecommunications Equipment: Changing Markets and Trade Structures. OECD Publishing. p. 16. ISBN 9789264135536.
4. "Why Buy Refurbished Telecom Equipment?". DTC International Ltd. 20 March 2015. Retrieved 27 March 2015.
5. "Modem entry".
6. IEEE History Center. "Gottfried Ungerboeck Oral History". Archived from the original on June 25, 2007. Retrieved 2008-02-10.
7. Held, Gilbert (2000). Understanding Data Communications: From Fundamentals to Networking Third Edition. New York: John Wiley & Sons Ltd. pp. 68–69.
8. Greenstein, Shane; Stango, Victor (2006). Standards and Public Policy. Cambridge University Press. pp. 129–132. ISBN 978-1-139-46075-0.
9. "V.92 - News & Updates". November and October 2000 updates. Retrieved 17 September 2012.
10. "Modem compression: V.44 against V.42bis". Digit-life.com. Retrieved 2014-02-10.
11. Re: Modems FAQ at the Wayback Machine (archived January 4, 2007) - Wolfgang Henke.[dead link]
12. tsbmail (2011-04-15). "Data communication over the telephone network". Itu.int. Retrieved 2014-02-10.
13. "29.2 Historical Modem Protocols". tldp.org. Retrieved 2014-02-10.
14. "concordia.ca — Data Communication and Computer Networks"(PDF). Retrieved 2014-02-10.
15. "Group 3 Facsimile Communication". garretwilson.com. 2013-09-20. Retrieved 2014-02-10.
16. "upatras.gr - Implementation of a V.34 modem on a Digital Signal Processor" (PDF). Retrieved 2014-02-10.
17. Jones, Les. "Bonding: 112K, 168K, and beyond". 56K.COM.[dead link]
18. Suzanne Choney. "AOL still has 3.5 million dial-up subscribers - Technology on NBCNews.com". Wayback.archive.org. Retrieved 2014-02-10.
19. "What is a USB modem?". Vergelijkmobielinternet.nl. Retrieved 17 September 2012.[dead link]
20. "HUAWEI E1762,HSPA/UMTS 900/2100 Support 2Mbps (5.76Mbps ready) HSUPA and 7.2Mbps HSDPA services". 3gmodem.com.hk. Retrieved 2013-04-22.
21. "Sierra Wireless Compass 885 HSUPA 3G modem". The Register. Retrieved 2014-02-10.
22. Lawson, Stephen (May 2, 2011). "Laptop Users Still Prefer USB Modems". PCWorld. IDG Consumer & SMB. Retrieved 2016-08-13.
23. Michel, Stephanie (September 19, 2013). "Which optical modulation scheme best fits my application?". LIGHTWAVE.

24. Michael Kassner (February 10, 2015). "Researchers double throughput of long-distance fiber optics". TechRepublic.
25. Bengt-Erik Olsson; Anders Djupsjöbacka; Jonas Mårtensson; Arne Alping (6 Dec 2011). "112 Gbit/s RF-assisted dual carrier DP-16-QAM transmitter using optical phase modulator" (PDF). OPTICS EXPRESS. Optical Society of America.
26. Stephen Hardy (March 17, 2016). "ClariPhy targets 400G with new 16-nm DSP silicon". LIGHTWAVE.
27. "ClariPhy Shatters Fiber and System Capacity Barriers with Industry's First 16nm Coherent Optical Networking Platform". optics.org. 17 Mar 2016.
28. "Nokia Bell Labs achieve 65 Terabit-per-second transmission record for transoceanic cable systems". Noika. 12 October 2016.
29. "router". Oxford English Dictionary (3rd ed.). Oxford University Press. September 2005. (Subscription or UK public library membershiprequired.)
30. "Overview Of Key Routing Protocol Concepts: Architectures, Protocol Types, Algorithms and Metrics". Tcpipguide.com. Retrieved 15 January 2011.
31. "Cisco Networking Academy's Introduction to Routing Dynamically". Cisco. Retrieved August 1, 2015.
32. Requirements for IPv4 Routers,RFC 1812, F. Baker, June 1995
33. Requirements for Separation of IP Control and Forwarding,RFC 3654, H. Khosravi & T. Anderson, November 2003
34. "Setting uo Netflow on Cisco Routers". MY-Technet.com date unknown. Retrieved 15 January 2011.
35. "Windows Home Server: Router Setup". Microsoft Technet 14 Aug 2010. Retrieved 15 January 2011.
36. Oppenheimer, Pr (2004). Top-Down Network Design. Indianapolis: Cisco Press. ISBN 1-58705-152-4.
37. "Windows Small Business Server 2008: Router Setup". Microsoft Technet Nov 2010. Retrieved 15 January 2011.
38. See "Network Address Translation (NAT) FAQ".
39. Cf. "RFC 3022 – Traditional IP Network Address Translator (Traditional NAT)".
40. But see "Security Considerations Of NAT" (PDF). University of Michigan. Archived from the original (PDF) on October 18, 2014., which argues that NAT is not a security feature.
41. Global Internet Experts Reveal Plan for More Secure, Reliable Wi-Fi Routers - and Internet
42. "Core Network Planning". Microsoft Technet May 28, 2009. Retrieved 15 January 2011.
43. H. Berkowitz; et al. (June 2005), Terminology for Benchmarking BGP Device Convergence in the Control Plane, RFC 4098

44. "M160 Internet Backbone Router" (PDF). Juniper Networks Date unknown. Retrieved 15 January 2011.
45. "Virtual Backbone Routers" (PDF). IronBridge Networks, Inc. September, 2000. Retrieved 15 January 2011.
46. BGP/MPLS VPNs,RFC 2547, E. Rosen and Y. Rekhter, April 2004
47. Davies, Shanks, Heart, Barker, Despres, Detwiler and Riml, "Report of Subgroup 1 on Communication System", INWG Note No. 1.
48. Vinton Cerf, Robert Kahn, "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Volume 22, Issue 5, May 1974, pp. 637 - 648.
49. David Boggs, John Shoch, Edward Taft, Robert Metcalfe, "Pup: An Internetwork Architecture", IEEE Transactions on Communications, Volume 28, Issue 4, April 1980, pp. 612- 624.
50. Craig Partridge, S. Blumenthal, "Data networking at BBN"; IEEE Annals of the History of Computing, Volume 28, Issue 1; January–March 2006.
51. Valley of the Nerds: Who Really Invented the Multiprotocol Router, and Why Should We Care?, Public Broadcasting Service, Accessed August 11, 2007.
52. Router Man, NetworkWorld, Accessed June 22, 2007.
53. David D. Clark, "M.I.T. Campus Network Implementation", CCNG-2, Campus Computer Network Group, M.I.T., Cambridge, 1982; pp. 26.
54. Pete Carey, "A Start-Up's True Tale: Often-told story of Cisco's launch leaves out the drama, intrigue", San Jose Mercury News, December 1, 2001.
55. Roberts, Lawrence (22 July 2003). "The Next Generation of IP - Flow Routing". Retrieved 22 February 2015.
56. David Davis (Apr 19, 2007). "Cisco administration 101: What you need to know about default routes".
57. Diane Teare (Mar 2013). Implementing Cisco IP Routing (ROUTE): Foundation Learning Guide. Cisco Press. pp. 330–334.
58. Diane Teare (Mar 2013). "Chapter 5: Implementing Path Control". Implementing Cisco IP Routing (ROUTE): Foundation Learning Guide. Cisco Press. pp. 330–334.

CHAPTER 9

# World Wide Web

## Chapter Contents

- **Introduction**
- **Analogue Switch**
- **Transmission Line**
- **Modem**
- **Router (Computing)**

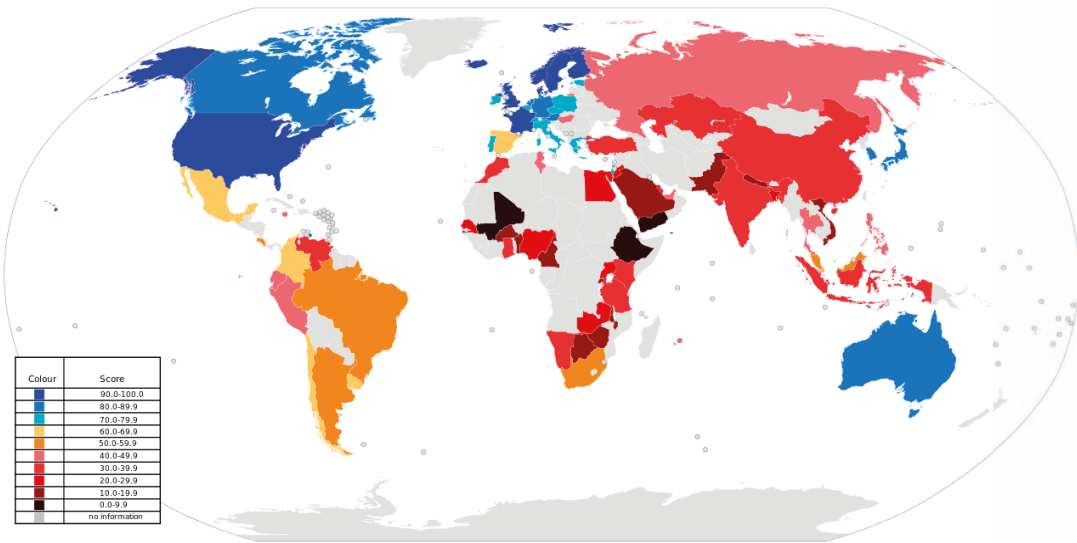
The Internet and the World Wide Web (WWW or Web) are not the same thing, though they are related. The Internet encompasses the Web, but it also encompasses other online protocols in addition to the Web. In basic terms, the difference is that the former is a massive system of connected international networks, while the latter is one type of service available within that network.

## INTRODUCTION

The World Wide Web (abbreviated WWW or the Web) is an information space where documents and other web resources are identified by Uniform Resource Locators (URLs), interlinked by hypertext links, and can be accessed via the Internet. English scientist Tim Berners-Lee invented the World Wide Web in 1989. He wrote the first web browser computer programme in 1990 while employed at CERN in Switzerland.

The World Wide Web has been central to the development of the Information Age and is the primary tool billions of people use to interact on the Internet. Web pages are primarily text documents formatted and annotated with Hypertext Markup Language (HTML). In addition to formatted text, web pages may contain images, video, audio, and software components that are rendered in the user's web browser as coherent pages of multimedia content. Embedded hyperlinks permit users to navigate between web pages.

Multiple web pages with a common theme, a common domain name, or both, make up a website. Website content can largely be provided by the publisher, or interactive where users contribute content or the content depends upon the user or their actions. Websites may be mostly informative, primarily for entertainment, or largely for commercial, governmental, or non-governmental organisational purposes. In the 2006 Great British Design Quest organised by the BBC and the Design Museum, the World Wide Web was voted among the top 10 British design icons.




A global map showing the availability of the World Wide Web in the 2010s. The regions with the highest level of access, in dark blue, are North America, Europe, Japan and Australia.

Tim Berners-Lee's vision of a global hyperlinked information system became a possibility by the second half of the 1980s. By 1985, the global Internet began to proliferate in Europe and in the Domain Name System (upon which the Uniform Resource Locator is built) came into being. In 1988 the first direct IP connection between Europe and North America was made and Berners-Lee began to openly discuss the possibility of a web-like system at CERN. In March 1989 Berners-Lee issued a proposal to the management at CERN for a system called "Mesh" that referenced ENQUIRE, a database and software project he had built in 1980, which used the term "web" and described a more elaborate information management system based on links embedded in readable text: "Imagine, then, the references in this document all being associated with the network address of the thing to which they referred, so that while reading this document you could skip to them with a click of the mouse." Such a system, he explained, could be referred to using one of the existing meanings of the word *hypertext*, a term that he says was coined in the 1950s. There is no reason, the proposal continues, why such hypertext links could not encompass multimedia documents including graphics, speech and video, so that Berners-Lee goes on to use the term *hypermedia*.



The NeXT Computer used by Tim Berners-Lee at CERN.



The corridor where WWW was born. CERN, ground floor of building No.1

With help from his colleague and fellow hypertext enthusiast Robert Cailliau he published a more formal proposal on 12 November 1990 to build a "Hypertext project" called "WorldWideWeb" (one word) as a "web" of "hypertext documents" to be viewed by "browsers" using a client–server architecture. At this point HTML and HTTP had already been in development for about two months and the first Web server was about a month from completing its first successful test. This proposal estimated that a read-only web would be developed within three months and that it would take six months to achieve "the creation of new links and new material by readers, authorship becomes universal" as well as "the automatic notification of a reader when new material of interest to him/her has become available." While the read-only goal was met, accessible authorship of web content took longer to mature, with the wiki concept, WebDAV, blogs, Web 2.0 and RSS/Atom.

## HISTORY OF THE WORLD WIDE WEB

The World Wide Web ("WWW" or simply the "Web") is a global information medium which users can read and write via computers connected to the Internet. The term is often mistakenly used as a synonym for the Internet itself, but the Web is a service that operates over the Internet, just as e-mail also does. The history of the Internet dates back significantly further than that of the World Wide Web.



The web's logo designed by Robert Cailliau

### Precursors

The hypertext portion of the Web in particular has an intricate intellectual history; notable influences and precursors include Vannevar Bush's Memex, IBM's Generalized Markup Language, and Ted Nelson's Project Xanadu.

Paul Otlet's Mundaneum project has also been named as an early 20th century precursor of the Web.

The concept of a global information system connecting homes is prefigured in "A Logic Named Joe", a 1946 short story by Murray Leinster, in which computer terminals, called "logics," are present in every home. Although the computer system in the story is centralized, the story anticipates a ubiquitous information environment similar to the Web.

## 1980–1991: Invention and Implementation of the Web




The NeXTcube used by Tim Berners-Lee at CERN became the first Web server.

In 1980, Tim Berners-Lee, an English independent contractor at the European Organization for Nuclear Research (CERN) in Switzerland, built ENQUIRE, as a personal database of people and software models, but also as a way to play with hypertext; each new page of information in ENQUIRE had to be linked to an existing page.

Berners-Lee's contract in 1980 was from June to December, but in 1984 he returned to CERN in a permanent role, and considered its problems of information management: physicists from around the world needed to share data, yet they lacked common machines and any shared presentation software.

Shortly after Berners-Lee's return to CERN, TCP/IP protocols were installed on some key non-Unix machines at the institution, turning it into the largest Internet site in Europe within a few years. As a result, CERN's infrastructure was ready for Berners-Lee to create the Web.

Berners-Lee wrote a proposal in March 1989 for "a large hypertext database with typed links". Although the proposal attracted little interest, Berners-Lee was encouraged by his boss, Mike Sendall, to begin implementing his system on a newly acquired NeXT workstation. He considered several names, including *Information Mesh*, *The Information Mine* or *Mine of Information*, but settled on *World Wide Web*.

Berners-Lee found an enthusiastic supporter in Robert Cailliau. Berners-Lee and Cailliau pitched Berners-Lee's ideas to the European Conference on Hypertext Technology in September 1990, but found no vendors who could appreciate his vision of marrying hypertext with the Internet.

By Christmas 1990, Berners-Lee had built all the tools necessary for a working Web: the HyperText Transfer Protocol (HTTP) 0.9, the HyperText Markup Language (HTML), the first Web browser (named WorldWideWeb, which was also a Web editor), the first HTTP server software (later known as CERN httpd), the first web server (http://info.cern.ch), and the first Web pages that described the project itself. The browser could access Usenet newsgroups and FTP files as well. However, it could run only on the NeXT; Nicola Pellow therefore created a simple text browser that could run on almost any computer called the Line Mode Browser. To encourage use within CERN, Bernd Pollermann put the CERN telephone directory on the web — previously users had to log onto the mainframe in order to look up phone numbers.

While inventing and working on setting up the Web, Berners-Lee spent most of his working hours in Building 31 at CERN (46.2325°N 6.0450°E), but also at his two homes, one in France, one in Switzerland. In January 1991 the first Web servers outside CERN itself were switched on.

The first web page may be lost, but Paul Jones of UNC-Chapel Hill in North Carolina revealed in May 2013 that he has a copy of a page sent to him in 1991 by Berners-Lee which is the oldest known web page. Jones stored the plain-text page, with hyperlinks, on a floppy disk and on his NeXT computer. CERN put the oldest known web page back online in 2014, complete with hyperlinks that helped users get started and helped them navigate what was then a very small web.

On August 6, 1991, Berners-Lee posted a short summary of the World Wide Web project on the alt.hypertext newsgroup, inviting collaborators. This date is sometimes confused with the public availability of the first web servers, which had occurred months earlier.

Paul Kunz from the Stanford Linear Accelerator Center visited CERN in September 1991, and was captivated by the Web. He brought the NeXT software back to SLAC, where librarian Louise Addis adapted it for the VM/CMS operating system on the IBM mainframe as a way to display SLAC's catalog of online documents; this was the first web server outside of Europe and the first in North America. The www-talk mailing list was started in the same month.

An early CERN-related contribution to the Web was the parody band Les Horribles Cernettes, whose promotional image is believed to be among the Web's first five pictures.

## 1992–1995: Growth of the Web

In keeping with its birth at CERN and the first page opened, early adopters of the World Wide Web were primarily university-based scientific departments or physics laboratories such as Fermilab and SLAC. By January 1993 there were fifty Web servers across the world; by October 1993 there were over five hundred. Two of the earliest webcomics started on the World Wide Web in 1993: *Doctor Fun* and *NetBoy*.

Early websites intermingled links for both the HTTP web protocol and the then-popular Gopher protocol, which provided access to content through hypertext menus presented as a file system rather than through HTML files. Early Web users would navigate either by bookmarking popular directory pages, such as Berners-Lee's first site at http://info.cern.ch/, or by consulting updated lists such as the NCSA "What's New" page. Some sites were also indexed by WAIS, enabling users to submit full-text searches similar to the capability later provided by search engines.

By the end of 1994, the total number of websites was still minute compared to present figures, but quite a number of notable websites were already active, many of which are the precursors or inspiring examples of today's most popular services.

## Early Browsers

Initially, a web browser was available only for the NeXT operating system. This shortcoming was discussed in January 1992, and alleviated in April 1992 by the release of Erwise, an application developed at the Helsinki University of Technology, and in May by ViolaWWW, created by Pei-Yuan Wei, which included advanced features such as embedded graphics, scripting, and animation. ViolaWWW was originally an application for HyperCard. Both programs ran on the X Window System for Unix.

Students at the University of Kansas adapted an existing text-only hypertext browser, Lynx, to access the web. Lynx was available on Unix and DOS, and some web designers, unimpressed with glossy graphical websites, held that a website not accessible through Lynx wasn't worth visiting.

The first Microsoft Windows browser was Cello, written by Thomas R. Bruce for the Legal Information Institute at Cornell Law School to provide legal information, since access to Windows was more widespread amongst lawyers than access to Unix. Cello was released in June 1993.

The Web was first popularized by Mosaic, a graphical browser launched in 1993 by Marc Andreessen's team at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign (UIUC). The origins of Mosaic date to 1992. In November 1992, the NCSA at the University of Illinois (UIUC) established a website. In December 1992, Andreessen and Eric Bina, students attending UIUC and working at the NCSA, began work on Mosaic with funding from the High-Performance Computing and Communications Initiative, a US-federal research and development program. Andreessen and Bina released a Unix version of the browser in February 1993; Mac and Windows versions followed in August 1993. The browser gained popularity due to its strong support of integrated multimedia, and the authors' rapid response to user bug reports and recommendations for new features.

After graduation from UIUC, Andreessen and James H. Clark, former CEO of Silicon Graphics, met and formed Mosaic Communications Corporation in April 1994, to develop the Mosaic Netscape browser commercially. The company later changed its name to Netscape, and the browser was developed further as Netscape Navigator.

### *Web Governance*

In May 1994, the first International WWW Conference, organized by Robert Cailliau, was held at CERN; the conference has been held every year since. In April 1993, CERN had agreed that anyone could use the Web protocol and code royalty-free; this was in part a reaction to the perturbation caused by the University of Minnesota's announcement that it would begin charging license fees for its implementation of the Gopher protocol.

In September 1994, Berners-Lee founded the World Wide Web Consortium (W3C) at the Massachusetts Institute of Technology with support from the Defense Advanced Research Projects Agency (DARPA) and the European Commission. It comprised various companies that were willing to create standards and recommendations to improve the quality of the Web. Berners-Lee made the Web available freely, with no patent and no royalties due. The W3C decided that its standards must be based on royalty-free technology, so they can be easily adopted by anyone.

## 1996–1998: Commercialization of the Web

By 1996 it became obvious to most publicly traded companies that a public Web presence was no longer optional. Though at first people saw mainly the possibilities of free publishing and instant worldwide information, increasing familiarity with two-way communication over the "Web" led to the possibility of direct Web-based commerce (e-commerce) and instantaneous group communications worldwide. More dotcoms, displaying products on hypertext webpages, were added into the Web.

## 1999–2001: "Dot-Com" Boom and Bust

Low interest rates in 1998–99 facilitated an increase in start-up companies. Although a number of these new entrepreneurs had realistic plans and administrative ability, most of them lacked these characteristics but were able to sell their ideas to investors because of the novelty of the dot-com concept.

Historically, the dot-com boom can be seen as similar to a number of other technology-inspired booms of the past including railroads in the 1840s, automobiles in the early 20th century, radio in the 1920s, television in the 1940s, transistor electronics in the 1950s, computer time-sharing in the 1960s, and home computers and biotechnology in the 1980s.

In 2001 the bubble burst, and many dot-com startups went out of business after burning through their venture capital and failing to become profitable. Many others, however, did survive and thrive in the early 21st century. Many companies which began as online retailers blossomed and became highly profitable. More conventional retailers found online merchandising to be a profitable additional source of revenue. While some online entertainment and news outlets failed when their seed capital ran out, others persisted and eventually became economically self-sufficient. Traditional media outlets (newspaper publishers, broadcasters and cablecasters in particular) also found the Web to be a useful and profitable additional channel for content distribution, and an additional means to generate advertising revenue. The sites that survived and eventually prospered

after the bubble burst had two things in common; a sound business plan, and a niche in the marketplace that was, if not unique, particularly well-defined and well-served.

## 2002–Present: The Web Becomes Ubiquitous

In the aftermath of the dot-com bubble, telecommunications companies had a great deal of overcapacity as many Internet business clients went bust. That, plus ongoing investment in local cell infrastructure kept connectivity charges low, helped to make high-speed Internet connectivity more affordable. During this time, a handful of companies found success developing business models that helped make the World Wide Web a more compelling experience. These include airline booking sites, Google's search engine and its profitable approach to keyword-based advertising, as well as eBay's auction site and Amazon.com's online department store.

This new era also begot social networking websites, such as MySpace and Facebook, which gained acceptance rapidly and became a central part of youth culture.

### *Web 2.0*

Beginning in 2002, new ideas for sharing and exchanging content ad hoc, such as Weblogs and RSS, rapidly gained acceptance on the Web. This new model for information exchange, primarily featuring user-generated and user-edited websites, was dubbed Web 2.0. The Web 2.0 boom saw many new service-oriented startups catering to a newly democratized Web.

As the Web became easier to query, it attained a greater ease of use overall and gained a sense of organization which ushered in a period of rapid popularization. Many new sites such as Wikipedia and its sister projects were based on the concept of user edited content. In 2005, three former PayPal employees created a video viewing website called YouTube, which became popular quickly and introduced a new concept of user-submitted content in major events.

The popularity of YouTube, Facebook, etc., combined with the increasing availability and affordability of high-speed connections has made video content far more common on all kinds of websites. Many video-content hosting and creation sites provide an easy means for their videos to be embedded on third party websites without payment or permission.

This combination of more user-created or edited content, and easy means of sharing content, such as via RSS widgets and video embedding, has led to many sites with a typical "Web 2.0" feel. They have articles with embedded video, user-submitted comments below the article, and RSS boxes to the side, listing some of the latest articles from other sites.

Continued extension of the Web has focused on connecting devices to the Internet, coined Intelligent Device Management. As Internet connectivity becomes ubiquitous, manufacturers have started to leverage the expanded computing power of their devices to enhance their usability and capability. Through Internet connectivity, manufacturers are now able to interact with the devices they have sold and shipped to their customers, and customers are able to interact with the manufacturer (and other providers) to access new content.

"Web 2.0" has found a place in the English lexicon.

## The semantic Web

Popularized by Berners-Lee's book *Weaving the Web* and a *Scientific American* article by Berners-Lee, James Hendler, and Ora Lassila, the term Semantic Web describes an evolution of the existing Web in which the network of hyperlinked human-readable web pages is extended by machine-readable metadata about documents and how they are related to each other, enabling automated agents to access the Web more intelligently and perform tasks on behalf of users. This has yet to happen. In 2006, Berners-Lee and colleagues stated that the idea "remains largely unrealized".



The CERN data centre in 2010 housing some WWW servers

The proposal was modelled after the SGML reader Dynatext by Electronic Book Technology, a spin-off from the Institute for Research in Information and Scholarship at Brown University. The Dynatext system, licensed by CERN, was a key player in the extension of SGML ISO 8879:1986 to Hypermedia within HyTime, but it was considered too expensive and had an inappropriate licensing policy for use in the general high energy physics community, namely a fee for each document and each document alteration. A NeXT Computer was used by Berners-Lee as the world's first web server and also to write the first web browser, WorldWideWeb, in 1990. By Christmas 1990, Berners-Lee had built all the tools necessary for a working Web: the first web browser (which was a web editor as well) and the first web server. The first web site, which described the project itself, was published on 20 December 1990.

The first web page may be lost, but Paul Jones of UNC-Chapel Hill in North Carolina announced in May 2013 that Berners-Lee gave him what he says is the oldest known web page during a 1991 visit to UNC. Jones stored it on a magneto-optical drive and on his

NeXT computer. On 6 August 1991, Berners-Lee published a short summary of the World Wide Web project on the newsgroup *alt.hypertext*. This date is sometimes confused with the public availability of the first web servers, which had occurred months earlier. As another example of such confusion, several news media reported that the first photo on the Web was published by Berners-Lee in 1992, an image of the CERN house band Les Horribles Cernettes taken by Silvano de Gennaro; Gennaro has disclaimed this story, writing that media were "totally distorting our words for the sake of cheap sensationalism."

The first server outside Europe was installed at the Stanford Linear Accelerator Center (SLAC) in Palo Alto, California, to host the SPIRES-HEP database. Accounts differ substantially as to the date of this event. The World Wide Web Consortium's timeline says December 1992, whereas SLAC itself claims December 1991, as does a W3C document titled *A Little History of the World Wide Web*. The underlying concept of hypertext originated in previous projects from the 1960s, such as the Hypertext Editing System (HES) at Brown University, Ted Nelson's Project Xanadu, and Douglas Engelbart's oN-Line System (NLS). Both Nelson and Engelbart were in turn inspired by Vannevar Bush's microfilm-based *memex*, which was described in the 1945 essay "As We May Think".

Berners-Lee's breakthrough was to marry hypertext to the Internet. In his book *Weaving The Web*, he explains that he had repeatedly suggested that a marriage between the two technologies was possible to members of *both* technical communities, but when no one took up his invitation, he finally assumed the project himself. In the process, he developed three essential technologies:

- a system of globally unique identifiers for resources on the Web and elsewhere, the universal document identifier (UDI), later known as uniform resource locator (URL) and uniform resource identifier (URI);
- the publishing language HyperText Markup Language (HTML);
- the Hypertext Transfer Protocol (HTTP).

The World Wide Web had a number of differences from other hypertext systems available at the time. The Web required only unidirectional links rather than bidirectional ones, making it possible for someone to link to another resource without action by the owner of that resource. It also significantly reduced the difficulty of implementing web servers and browsers (in comparison to earlier systems), but in turn presented the chronic problem of *link rot*. Unlike predecessors such as HyperCard, the World Wide Web was non-proprietary, making it possible to develop servers and clients independently and to add extensions without licensing restrictions. On 30 April 1993, CERN announced that the World Wide Web would be free to anyone, with no fees due. Coming two months after the announcement that the server implementation of the Gopher protocol was no longer free to use, this produced a rapid shift away from Gopher and towards the Web. An early popular web browser was ViolaWWW for Unix and the X Windowing System.



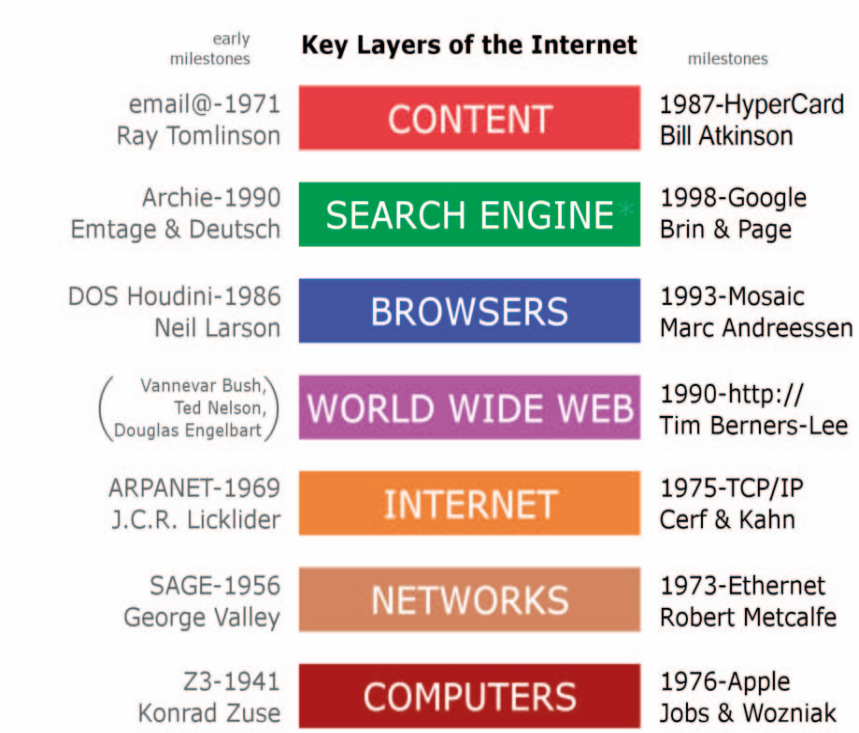
Robert Cailliau, Jean-François Abramatic formerly of INRIA, and Tim Berners-Lee at the 10th anniversary of the World Wide Web Consortium.

Scholars generally agree that a turning point for the World Wide Web began with the introduction of the Mosaic web browser in 1993, a graphical browser developed by a team at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign (NCSA-UIUC), led by Marc Andreessen. Funding for Mosaic came from the U.S. *High-Performance Computing and Communications Initiative* and the *High Performance Computing and Communication Act of 1991*, one of several computing developments initiated by U.S. Senator Al Gore. Prior to the release of Mosaic, graphics were not commonly mixed with text in web pages and the web's popularity was less than older protocols in use over the Internet, such as Gopher and Wide Area Information Servers (WAIS). Mosaic's graphical user interface allowed the Web to become, by far, the most popular Internet protocol. The World Wide Web Consortium (W3C) was founded by Tim Berners-Lee after he left the European Organization for Nuclear Research (CERN) in October 1994. It was founded at the Massachusetts Institute of Technology Laboratory for Computer Science (MIT/LCS) with support from the Defense Advanced Research Projects Agency (DARPA), which had pioneered the Internet; a year later, a second site was founded at INRIA (a French national computer research lab) with support from the European Commission DG InfSo; and in 1996, a third continental site was created in Japan at Keio University. By the end of 1994, the total number of websites was still relatively small, but many notable websites were already active that foreshadowed or inspired today's most popular services.

Connected by the Internet, other websites were created around the world. This motivated international standards development for protocols and formatting. Berners-Lee continued to stay involved in guiding the development of web standards, such as the markup languages to compose web pages and he advocated his vision of a Semantic Web. The World Wide Web enabled the spread of information over the Internet through

an easy-to-use and flexible format. It thus played an important role in popularising use of the Internet. Although the two terms are sometimes conflated in popular use, *World Wide Web* is not synonymous with *Internet*. The Web is an information space containing hyperlinked documents and other resources, identified by their URIs. It is implemented as both client and server software using Internet protocols such as TCP/IP and HTTP. Berners-Lee was knighted in 2004 by Queen Elizabeth II for "services to the global development of the Internet".

## Function




The World Wide Web functions as an application layer protocol that is run "on top of" (figuratively) the Internet, helping to make it more functional. The advent of the Mosaic web browser helped to make the web much more usable, to include the display of images and moving images (gifs).

The terms *Internet* and *World Wide Web* are often used without much distinction. However, the two are not the same. The Internet is a global system of interconnected computer networks. In contrast, the World Wide Web is a global collection of documents and other resources, linked by hyperlinks and URIs. Web resources are usually accessed using HTTP, which is one of many Internet communication protocols.

Viewing a web page on the World Wide Web normally begins either by typing the URL of the page into a web browser, or by following a hyperlink to that page or resource. The web browser then initiates a series of background communication messages

to fetch and display the requested page. In the 1990s, using a browser to view web pages—and to move from one web page to another through hyperlinks—came to be known as ‹browsing,' ‹web surfing' (after channel surfing), or ‹navigating the Web'. Early studies of this new behaviour investigated user patterns in using web browsers. One study, for example, found five user patterns: exploratory surfing, window surfing, evolved surfing, bounded navigation and targeted navigation.

The following example demonstrates the functioning of a web browser when accessing a page at the URL http://www.example.org/home.html. The browser resolves the server name of the URL (www.example.org) into an Internet Protocol address using the globally distributed Domain Name System (DNS). This lookup returns an IP address such as *203.0.113.4* or *2001:db8:2e::7334*. The browser then requests the resource by sending an HTTP request across the Internet to the computer at that address. It requests service from a specific TCP port number that is well known for the HTTP service, so that the receiving host can distinguish an HTTP request from other network protocols it may be servicing. The HTTP protocol normally uses port number 80. The content of the HTTP request can be as simple as two lines of text:

```
GET /home.html HTTP/1.1
Host: www.example.org
```

The computer receiving the HTTP request delivers it to web server software listening for requests on port 80. If the web server can fulfil the request it sends an HTTP response back to the browser indicating success:

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=UTF-8
```

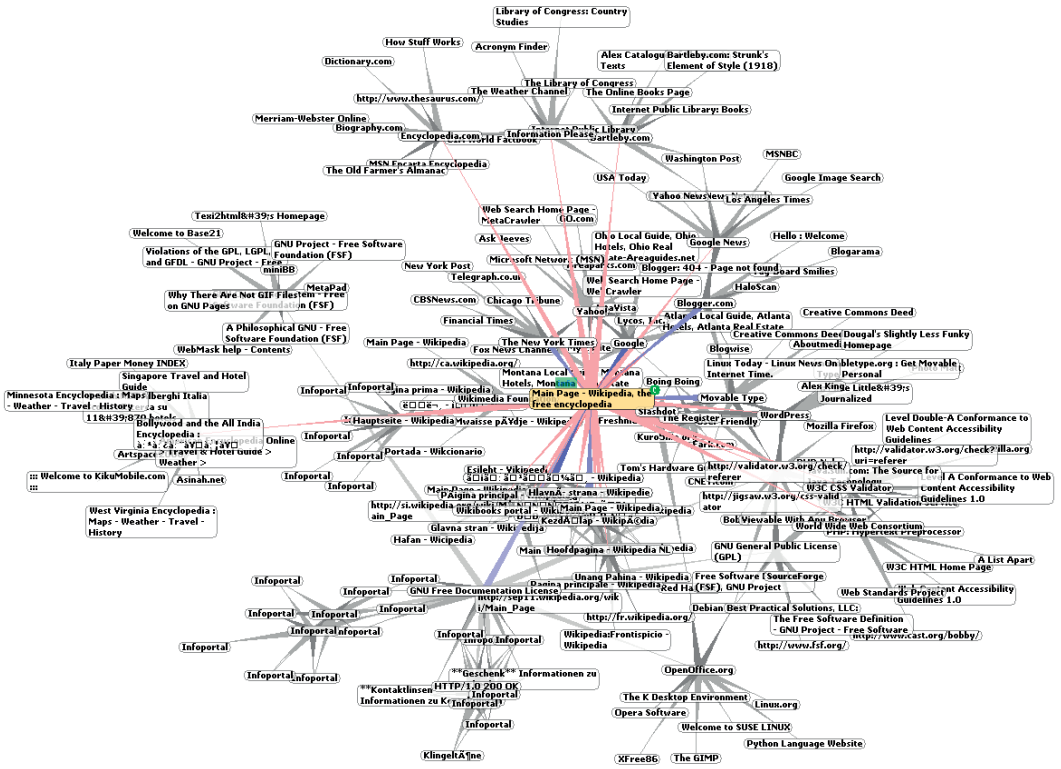
followed by the content of the requested page. HyperText Markup Language (HTML) for a basic web page might look like this:

```
<html>
  <head>
    <title>Example.org – The World Wide Web</title>
  </head>
  <body>
    <p>The World Wide Web, abbreviated as WWW and commonly known ...</p>
  </body>
</html>
```

The web browser parses the HTML and interprets the markup (<**title**>, <**p**> for paragraph, and such) that surrounds the words to format the text on the screen. Many web pages use HTML to reference the URLs of other resources such as images, other embedded media, scripts that affect page behaviour, and Cascading Style Sheets that affect page layout. The browser makes additional HTTP requests to the web server for these other Internet media types. As it receives their content from the web server, the browser progressively renders the page onto the screen as specified by its HTML and these additional resources.

## *Linking*

Most web pages contain hyperlinks to other related pages and perhaps to downloadable files, source documents, definitions and other web resources. In the underlying HTML, a hyperlink looks like this: <**a** href=”http://www.example.org/home.html”>Example.org Homepage</**a**>




Graphic representation of a minute fraction of the WWW, demonstrating hyperlinks

Such a collection of useful, related resources, interconnected via hypertext links is dubbed a *web* of information. Publication on the Internet created what Tim Berners-Lee first called the *WorldWideWeb* (in its original CamelCase, which was subsequently discarded) in November 1990.

The hyperlink structure of the WWW is described by the webgraph: the nodes of the webgraph correspond to the web pages (or URLs) the directed edges between them to the hyperlinks. Over time, many web resources pointed to by hyperlinks disappear, relocate, or are replaced with different content. This makes hyperlinks obsolete, a phenomenon referred to in some circles as link rot, and the hyperlinks affected by it are often called dead links. The ephemeral nature of the Web has prompted many efforts to archive web sites. The Internet Archive, active since 1996, is the best known of such efforts.

## Dynamic Updates of Web Pages

JavaScript is a scripting language that was initially developed in 1995 by Brendan Eich, then of Netscape, for use within web pages. The standardised version is ECMAScript. To make web pages more interactive, some web applications also use JavaScript techniques such as Ajax (asynchronous JavaScript and XML). Client-side script is delivered with the page that can make additional HTTP requests to the server, either in response to user actions such as mouse movements or clicks, or based on elapsed time. The server's responses are used to modify the current page rather than creating a new page with each response, so the server needs only to provide limited, incremental information. Multiple Ajax requests can be handled at the same time, and users can interact with the page while data is retrieved. Web pages may also regularly poll the server to check whether new information is available.

## WWW Prefix

Many hostnames used for the World Wide Web begin with *www* because of the long-standing practice of naming Internet hosts according to the services they provide. The hostname of a web server is often *www*, in the same way that it may be *ftp* for an FTP server, and *news* or *nntp* for a USENET news server. These host names appear as Domain Name System (DNS) or subdomain names, as in *www.example.com*. The use of *www* is not required by any technical or policy standard and many web sites do not use it; indeed, the first ever web server was called *nxoc01.cern.ch*. According to Paolo Palazzi, who worked at CERN along with Tim Berners-Lee, the popular use of *www* as subdomain was accidental; the World Wide Web project page was intended to be published at www.cern.ch while info.cern.ch was intended to be the CERN home page, however the DNS records were never switched, and the practice of prepending *www* to an institution's website domain name was subsequently copied. Many established websites still use the prefix, or they employ other subdomain names such as *www2*, *secure* or *en* for special purposes. Many such web servers are set up so that both the main domain name (e.g., example.com) and the *www* subdomain (e.g., www.example.com) refer to the same site; others require one form or the other, or they may map to different web sites. The use of a subdomain name is useful for load balancing incoming web traffic by creating a CNAME record that points to a cluster of web servers. Since, currently, only a subdomain can be used in a CNAME, the same result cannot be achieved by using the bare domain root.

When a user submits an incomplete domain name to a web browser in its address bar input field, some web browsers automatically try adding the prefix "www" to the beginning of it and possibly ".com", ".org" and ".net" at the end, depending on what might be missing. For example, entering ‹microsoft' may be transformed to *http://www.microsoft.com/* and 'openoffice' to *http://www.openoffice.org*. This feature started appearing in early versions of Mozilla Firefox, when it still had the working title 'Firebird' in early 2003, from an earlier practice in browsers such as Lynx It is reported that Microsoft was granted a US patent for the same idea in 2008, but only for mobile devices.

In English, *www* is usually read as *double-u double-u double-u*. Some users pronounce it *dub-dub-dub*, particularly in New Zealand. Stephen Fry, in his "Podgrammes" series of podcasts, pronounces it *wuh wuh wuh*. The English writer Douglas Adams once quipped

in *The Independent on Sunday* (1999): "The World Wide Web is the only thing I know of whose shortened form takes three times longer to say than what it's short for". In Mandarin Chinese, *World Wide Web* is commonly translated via a phono-semantic matching to *wàn wéi wǎng* , which satisfies *www* and literally means "myriad dimensional net", a translation that reflects the design concept and proliferation of the World Wide Web. Tim Berners-Lee's web-space states that *World Wide Web* is officially spelled as three separate words, each capitalised, with no intervening hyphens. Use of the www prefix has been declining, especially when Web 2.0 web applications sought to brand their domain names and make them easily pronounceable. As the mobile web grew in popularity, services like Gmail.com, Outlook.com, MySpace.com, Facebook.com and Twitter.com are most often mentioned without adding "www." (or, indeed, ".com") to the domain.

### Scheme Specifiers

The scheme specifiers *http://* and *https://* at the start of a web URI refer to Hypertext Transfer Protocol or HTTP Secure, respectively. They specify the communication protocol to use for the request and response. The HTTP protocol is fundamental to the operation of the World Wide Web, and the added encryption layer in HTTPS is essential when browsers send or retrieve confidential data, such as passwords or banking information. Web browsers usually automatically prepend http:// to user-entered URIs, if omitted.

## Web Security

For criminals, the Web has become a venue to spread malware and engage in a range of cybercrimes, including identity theft, fraud, espionage and intelligence gathering. Web-based vulnerabilities now outnumber traditional computer security concerns, and as measured by Google, about one in ten web pages may contain malicious code. Most web-based attacks take place on legitimate websites, and most, as measured by Sophos, are hosted in the United States, China and Russia. The most common of all malware threats is SQL injection attacks against websites. Through HTML and URIs, the Web was vulnerable to attacks like cross-site scripting (XSS) that came with the introduction of JavaScript and were exacerbated to some degree by Web 2.0 and Ajax web design that favours the use of scripts. Today by one estimate, 70% of all websites are open to XSS attacks on their users. Phishing is another common threat to the Web. "SA, the Security Division of EMC, today announced the findings of its January 2013 Fraud Report, estimating the global losses from phishing at $1.5 Billion in 2012". Two of the well-known phishing methods are Covert Redirect and Open Redirect.

Proposed solutions vary. Large security companies like McAfee already design governance and compliance suites to meet post-9/11 regulations, and some, like Finjan have recommended active real-time inspection of programming code and all content regardless of its source. Some have argued that for enterprises to see Web security as a business opportunity rather than a cost centre, while others call for "ubiquitous, always-on digital rights management" enforced in the infrastructure to replace the hundreds of companies that secure data and networks. Jonathan Zittrain has said users sharing responsibility for computing safety is far preferable to locking down the Internet.

## Privacy

Every time a client requests a web page, the server can identify the request's IP address and usually logs it. Also, unless set not to do so, most web browsers record requested web pages in a viewable *history* feature, and usually cache much of the content locally. Unless the server-browser communication uses HTTPS encryption, web requests and responses travel in plain text across the Internet and can be viewed, recorded, and cached by intermediate systems. When a web page asks for, and the user supplies, personally identifiable information—such as their real name, address, e-mail address, etc.—web-based entities can associate current web traffic with that individual. If the website uses HTTP cookies, username and password authentication, or other tracking techniques, it can relate other web visits, before and after, to the identifiable information provided. In this way it is possible for a web-based organisation to develop and build a profile of the individual people who use its site or sites. It may be able to build a record for an individual that includes information about their leisure activities, their shopping interests, their profession, and other aspects of their demographic profile. These profiles are obviously of potential interest to marketeers, advertisers and others. Depending on the website's terms and conditions and the local laws that apply information from these profiles may be sold, shared, or passed to other organisations without the user being informed. For many ordinary people, this means little more than some unexpected e-mails in their in-box, or some uncannily relevant advertising on a future web page. For others, it can mean that time spent indulging an unusual interest can result in a deluge of further targeted marketing that may be unwelcome. Law enforcement, counter terrorism and espionage agencies can also identify, target and track individuals based on their interests or proclivities on the Web.

Social networking sites try to get users to use their real names, interests, and locations, rather than pseudonyms. These website's leaders believe this makes the social networking experience more engaging for users. On the other hand, uploaded photographs or unguarded statements can be identified to an individual, who may regret this exposure. Employers, schools, parents, and other relatives may be influenced by aspects of social networking profiles, such as text posts or digital photos, that the posting individual did not intend for these audiences. On-line bullies may make use of personal information to harass or stalk users. Modern social networking websites allow fine grained control of the privacy settings for each individual posting, but these can be complex and not easy to find or use, especially for beginners. Photographs and videos posted onto websites have caused particular problems, as they can add a person's face to an on-line profile. With modern and potential facial recognition technology, it may then be possible to relate that face with other, previously anonymous, images, events and scenarios that have been imaged elsewhere. Because of image caching, mirroring and copying, it is difficult to remove an image from the World Wide Web.

## Standards

Many formal standards and other technical specifications and software define the operation of different aspects of the World Wide Web, the Internet, and computer information exchange. Many of the documents are the work of the World Wide Web Consortium

(W3C), headed by Berners-Lee, but some are produced by the Internet Engineering Task Force (IETF) and other organisations.

Usually, when web standards are discussed, the following publications are seen as foundational:

- Recommendations for markup languages, especially HTML and XHTML, from the W3C. These define the structure and interpretation of hypertext documents.
- Recommendations for stylesheets, especially CSS, from the W3C.
- Standards for ECMAScript (usually in the form of JavaScript), from Ecma International.
- Recommendations for the Document Object Model, from W3C.

Additional publications provide definitions of other essential technologies for the World Wide Web, including, but not limited to, the following:

- *Uniform Resource Identifier* (URI), which is a universal system for referencing resources on the Internet, such as hypertext documents and images. URIs, often called URLs, are defined by the IETF's RFC 3986 / STD 66: *Uniform Resource Identifier (URI): Generic Syntax*, as well as its predecessors and numerous URI scheme-defining RFCs;
- *HyperText Transfer Protocol (HTTP)*, especially as defined by RFC 2616: *HTTP/1.1* and RFC 2617: *HTTP Authentication*, which specify how the browser and server authenticate each other.

## Accessibility

There are methods for accessing the Web in alternative mediums and formats to facilitate use by individuals with disabilities. These disabilities may be visual, auditory, physical, speech-related, cognitive, neurological, or some combination. Accessibility features also help people with temporary disabilities, like a broken arm, or ageing users as their abilities change. The Web receives information as well as providing information and interacting with society. The World Wide Web Consortium claims that it is essential that the Web be accessible, so it can provide equal access and equal opportunity to people with disabilities. Tim Berners-Lee once noted, "The power of the Web is in its universality. Access by everyone regardless of disability is an essential aspect." Many countries regulate web accessibility as a requirement for websites. International cooperation in the W3C Web Accessibility Initiative led to simple guidelines that web content authors as well as software developers can use to make the Web accessible to persons who may or may not be using assistive technology.

## Internationalisation

The W3C Internationalisation Activity assures that web technology works in all languages, scripts, and cultures. Beginning in 2004 or 2005, Unicode gained ground and eventually in December 2007 surpassed both ASCII and Western European as the Web's most frequently used character encoding. Originally RFC 3986 allowed resources to be identified by URI in

a subset of US-ASCII. RFC 3987 allows more characters—any character in the Universal Character Set—and now a resource can be identified by IRI in any language.

## Statistics

Between 2005 and 2010, the number of web users doubled, and was expected to surpass two billion in 2010. Early studies in 1998 and 1999 estimating the size of the Web using capture/recapture methods showed that much of the web was not indexed by search engines and the Web was much larger than expected. According to a 2001 study, there was a massive number, over 550 billion, of documents on the Web, mostly in the invisible Web, or Deep Web. A 2002 survey of 2,024 million web pages determined that by far the most web content was in the English language: 56.4%; next were pages in German (7.7%), French (5.6%), and Japanese (4.9%). A more recent study, which used web searches in 75 different languages to sample the Web, determined that there were over 11.5 billion web pages in the publicly indexable web as of the end of January 2005. As of March 2009, the indexable web contains at least 25.21 billion pages. On 25 July 2008, Google software engineers Jesse Alpert and Nissan Hajaj announced that Google Search had discovered one trillion unique URLs. As of May 2009, over 109.5 million domains operated. Of these, 74% were commercial or other domains operating in the generic top-level domain *com*.Statistics measuring a website's popularity, such as the Alexa Internet rankings, are usually based either on the number of page views or on associated server "hits" (file requests) that it receives.

## Speed Issues

Frustration over congestion issues in the Internet infrastructure and the high latency that results in slow browsing, "freezing" of Web pages, and slow loading of websites has led to a pejorative name for the World Wide Web: the *World Wide Wait*. Speeding up the Internet is an ongoing discussion over the use of peering and QoS technologies. Other solutions to reduce the congestion can be found at W3C. Guidelines for web response times are:

- 0.1 second (one tenth of a second). Ideal response time. The user does not sense any interruption.
- 1 second. Highest acceptable response time. Download times above 1 second interrupt the user experience.
- 10 seconds. Unacceptable response time. The user experience is interrupted and the user is likely to leave the site or system.

## Web Caching

A web cache is a server computer located either on the public Internet, or within an enterprise that stores recently accessed web pages to improve response time for users when the same content is requested within a certain time after the original request. Most web browsers also implement a browser cache for recently obtained data, usually on the local

disk drive. HTTP requests by a browser may ask only for data that has changed since the last access. Web pages and resources may contain expiration information to control caching to secure sensitive data, such as in online banking, or to facilitate frequently updated sites, such as news media. Even sites with highly dynamic content may permit basic resources to be refreshed only occasionally. Web site designers find it worthwhile to collate resources such as CSS data and JavaScript into a few site-wide files so that they can be cached efficiently. Enterprise firewalls often cache Web resources requested by one user for the benefit of many users. Some search engines store cached content of frequently accessed websites.

## REFERENCES


1. "What is the difference between the Web and the Internet?". W3C Help and FAQ. W3C. 2009. Retrieved 16 July 2015.
2. McPherson, Stephanie Sammartino (2009). Tim Berners-Lee: Inventor of the World Wide Web. Twenty-First Century Books.
3. Quittner, Joshua (29 March 1999). "Network Designer Tim Berners-Lee". Time Magazine. Retrieved 17 May 2010. (subscription required (help)). He wove the World Wide Web and created a mass medium for the 21st century. The World Wide Web is Berners-Lee's alone. He designed it. He loosed it on the world. And he more than anyone else has fought to keep it open, nonproprietary and free.[page needed]
4. "World Wide Web Timeline". Pew Research Center. 11 March 2014. Retrieved 1 August 2015.
5. Dewey, Caitlin (12 March 2014). "36 Ways the Web Has Changed Us". The Washington Post. Retrieved 1 August 2015.
6. "Internet Live Stats". Retrieved 1 August 2015.
7. "Concorde voted the UK's top icon". BBC. 18 November 2016.
8. http://cs.wellesley.edu/~cs315/BOOKS/TBL12.pdf
9. Berners-Lee, Tim (March 1989). "Information Management: A Proposal". W3C. Retrieved 27 July 2009.
10. Berners-Lee, Tim; Cailliau, Robert (12 November 1990). "WorldWideWeb: Proposal for a HyperText Project". Retrieved 12 May 2015.
11. "Tim Berners-Lee's original World Wide Web browser". With recent phenomena like blogs and wikis, the Web is beginning to develop the kind of collaborative nature that its inventor envisaged from the start.
12. "Tim Berners-Lee: client". W3.org. Retrieved 27 July 2009.
13. "First Web pages". W3.org. Retrieved 27 July 2009.
14. "The birth of the web". CERN. Retrieved 23 December 2015.
15. Murawski, John (24 May 2013). "Hunt for world's oldest WWW page leads to UNC Chapel Hill". News & Observer.
16. "Short summary of the World Wide Web project". Google. 6 August 1991.

Retrieved 27 July 2009.

17. "Silvano de Gennaro disclaims 'the first photo on the Web'". Retrieved 27 July 2012. If you read well our website, it says that it was, to our knowledge, the 'first photo of a band'. Dozens of media are totally distorting our words for the sake of cheap sensationalism. Nobody knows which was the first photo on the Web.
18. "W3C timeline". Retrieved 30 March 2010.
19. "The Early World Wide Web at SLAC".
20. "About SPIRES". Retrieved 30 March 2010.
21. "A Little History of the World Wide Web".
22. Conklin, Jeff (1987), IEEE Computer, 20 (9), pp. 17–41
23. "Inventor of the Week Archive: The World Wide Web". Massachusetts Institute of Technology: MIT School of Engineering. Archived from the original on 8 June 2010. Retrieved 23 July 2009.
24. "Ten Years Public Domain for the Original Web Software". Tenyears-www.web.cern.ch. 30 April 2003. Retrieved 27 July 2009.
25. "Mosaic Web Browser History – NCSA, Marc Andreessen, Eric Bina". Livinginternet.com. Retrieved 27 July 2009.
26. "NCSA Mosaic – September 10, 1993 Demo". Totic.org. Retrieved 27 July 2009.
27. "Vice President Al Gore's ENIAC Anniversary Speech". Cs.washington.edu. 14 February 1996. Retrieved 27 July 2009.
28. "Internet legal definition of Internet". West's Encyclopedia of American Law, edition 2. Free Online Law Dictionary. 15 July 2009. Retrieved 25 November 2008.
29. "WWW (World Wide Web) Definition". TechTerms. Retrieved 19 February 2010.
30. Jacobs, Ian; Walsh, Norman (15 December 2004). "Architecture of the World Wide Web, Volume One". Introduction: W3C. Retrieved 11 February 2015.
31. "Supplement no.1, Diplomatic and Overseas List, K.B.E." (PDF). thegazette.co.uk. The Gazette. 31 December 2003. Retrieved 7 February 2016.
32. "Web's inventor gets a knighthood". BBC. 31 December 2003. Retrieved 25 May 2008.
33. "What is the difference between the Web and the Internet?". World Wide Web Consortium. Retrieved 18 April 2016.
34. Muylle, Steve; Rudy Moenaert; Marc Despont (1999). "A grounded theory of World Wide Web search behaviour". Journal of Marketing Communications. 5 (3): 143. doi:10.1080/135272699345644.
35. Hamilton, Naomi (31 July 2008). "The A-Z of Programming Languages: JavaScript". Computerworld. IDG. Retrieved 12 May 2009.
36. Buntin, Seth (23 September 2008). "jQuery Polling plugin". Retrieved 2009-08-22.
37. Berners-Lee, Tim. "Frequently asked questions by the Press". W3C. Retrieved 27 July 2009.

38. Palazzi, P (2011) 'The Early Days of the WWW at CERN'
39. "automatically adding www.___.com". mozillaZine. 16 May 2003. Retrieved 27 May 2009.
40. Masnick, Mike (7 July 2008). "Microsoft Patents Adding 'www.' And '.com' To Text". Techdirt. Retrieved 27 May 2009.
41. "Audible pronunciation of 'WWW'". Oxford University Press. Retrieved 25 May 2014.
42. Simonite, Tom (July 22, 2008). "Help us find a better way to pronounce www". newscientist.com. NewScientist, Technology. Retrieved 7 February 2016.
43. "MDBG Chinese-English dictionary – Translate". Retrieved 27 July 2009.
44. "Frequently asked questions by the Press – Tim BL". W3.org. Retrieved 27 July 2009.
45. Castelluccio, Michael (2010). "It's not your grandfather's Internet.". thefreelibrary.com. Institute of Management Accountants. Retrieved 7 February 2016.
46. Ben-Itzhak, Yuval (18 April 2008). "Infosecurity 2008 – New defence strategy in battle against e-crime". ComputerWeekly. Reed Business Information. Retrieved 20 April 2008.
47. Christey, Steve & Martin, Robert A. (22 May 2007). "Vulnerability Type Distributions in CVE (version 1.1)". MITRE Corporation. Retrieved 7 June 2008.
48. "Symantec Internet Security Threat Report: Trends for July–December 2007 (Executive Summary)" (PDF). XIII. Symantec Corp. April 2008: 1–2. Retrieved 11 May 2008.
49. "Google searches web's dark side". BBC News. 11 May 2007. Retrieved 26 April 2008.
50. "Security Threat Report (Q1 2008)" (PDF). Sophos. Retrieved 24 April 2008.
51. "Security threat report" (PDF). Sophos. July 2008. Retrieved 24 August 2008.
52. Fogie, Seth, Jeremiah Grossman, Robert Hansen, and Anton Rager (2007). Cross Site Scripting Attacks: XSS Exploits and Defense(PDF). Syngress, Elsevier Science & Technology. pp. 68–69, 127. ISBN 1-59749-154-3. Archived from the original (PDF) on 25 June 2008. Retrieved 6 June 2008.
53. O'Reilly, Tim (30 September 2005). "What Is Web 2.0". O'Reilly Media. pp. 4–5. Retrieved 4 June 2008. and AJAX web applications can introduce security vulnerabilities like "client-side security controls, increased attack surfaces, and new possibilities for Cross-Site Scripting (XSS)", in Ritchie, Paul (March 2007). "The security risks of AJAX/web 2.0 applications" (PDF). Infosecurity. Elsevier. Archived from the original (PDF) on 25 June 2008. Retrieved 6 June 2008. which cites Hayre, Jaswinder S. & Kelath, Jayasankar (22 June 2006). "Ajax Security Basics". SecurityFocus. Retrieved 6 June 2008.
54. Berinato, Scott (1 January 2007). "Software Vulnerability Disclosure: The Chilling Effect". CSO. CXO Media. p. 7. Archived from the original on 18 April 2008. Retrieved 7 June 2008.

55. "2012 Global Losses From phishing Estimated At $1.5 Bn". FirstPost. 20 February 2013. Retrieved 21 December 2014.
56. Prince, Brian (9 April 2008). "McAfee Governance, Risk and Compliance Business Unit". eWEEK. Ziff Davis Enterprise Holdings. Retrieved 25 April 2008.
57. Preston, Rob (12 April 2008). "Down To Business: It's Past Time To Elevate The Infosec Conversation". InformationWeek. United Business Media. Retrieved 25 April 2008.
58. Claburn, Thomas (6 February 2007). "RSA's Coviello Predicts Security Consolidation". InformationWeek. United Business Media. Retrieved 25 April 2008.
59. Duffy Marsan, Carolyn (9 April 2008). "How the iPhone is killing the 'Net". Network World. IDG. Retrieved 17 April 2008.
60. boyd, danah; Hargittai, Eszter (July 2010). "Facebook privacy settings: Who cares?". First Monday. University of Illinois at Chicago. 15 (8).
61. "Web Accessibility Initiative (WAI)". World Wide Web Consortium. Archived from the original on 2 April 2009. Retrieved 7 April 2009.
62. "Developing a Web Accessibility Business Case for Your Organization: Overview". World Wide Web Consortium. Retrieved 7 April 2009.
63. "Legal and Policy Factors in Developing a Web Accessibility Business Case for Your Organization". World Wide Web Consortium. Retrieved 7 April 2009.
64. "Web Content Accessibility Guidelines (WCAG) Overview". World Wide Web Consortium. Retrieved 7 April 2009.
65. "Internationalization (I18n) Activity". World Wide Web Consortium. Retrieved 10 April 2009.
66. Davis, Mark (5 April 2008). "Moving to Unicode 5.1". Google. Retrieved 10 April 2009.
67. "World Wide Web Consortium Supports the IETF URI Standard and IRI Proposed Standard" (Press release). World Wide Web Consortium. 26 January 2005. Retrieved 10 April 2009.
68. Lynn, Jonathan (19 October 2010). "Internet users to exceed 2 billion ...". Reuters. Retrieved 9 February 2011.
69. S. Lawrence, C.L. Giles, "Searching the World Wide Web," Science, 280(5360), 98–100, 1998.
70. S. Lawrence, C.L. Giles, "Accessibility of Information on the Web," Nature, 400, 107–109, 1999.
71. "The 'Deep' Web: Surfacing Hidden Value". Brightplanet.com. Archived from the original on 4 April 2008. Retrieved 27 July 2009.
72. "Distribution of languages on the Internet". Netz-tipp.de. Retrieved 27 July 2009.
73. Alessio Signorini. "The Indexable Web is More than 11.5 Billion Pages" (PDF). citeseerx.ist.psu.edu. Retrieved 4 February 2015.

74. "The size of the World Wide Web". Worldwidewebsize.com. Retrieved 27 July 2009.
75. Alpert, Jesse; Hajaj, Nissan (25 July 2008). "We knew the web was big...". The Official Google Blog.
76. "Domain Counts & Internet Statistics". Name Intelligence. Retrieved 17 May 2009.
77. "World Wide Wait". TechEncyclopedia. United Business Media. Retrieved 10 April 2009.
78. Khare, Rohit & Jacobs, Ian (1999). "W3C Recommendations Reduce 'World Wide Wait'". World Wide Web Consortium. Retrieved 10 April 2009.
79. Nielsen, Jakob (from Miller 1968; Card 1991) (1994). "5". Usability Engineering: Response Times: The Three Important Limits. Morgan Kaufmann. Retrieved 10 April 2009.

# Index


**A**

Advanced Research Projects Agency (ARPA) 2, 194
Advanced Research Projects Agency Network (ARPANET) 191
Asynchronous transfer mode (ATM) 87

**B**

Bolt, Beranek and Newman (BBN) 194
Broadcasting satellite service (BSS) 227
business television (BTV) 228
business-to-business (B2B) 23
business-to-consumer (B2C) 23

**C**

campus area network (CAN) 15
carrier sense multiple access with collision detection (CSMA/CD) 176
Communications satellite 221, 223, 225, 228, 229
Computer Science Network (CSNET) 192
constant bit rate (CBR) 92
Consultative Committee for Space Data Systems (CCSDS) 70
cross-site scripting (XSS) 271
cyclic redundancy check (CRC) 71

**D**

Defense Advanced Research Projects Agency (DARPA) 262, 266
Delay-tolerant networking (DTN) 46
Direct Multiplex Control (DMC) 195
Domain Name System (DNS) 268, 270

**F**

Federal Communications Commission (FCC) 51, 126
Fixed satellite service (FSS) 227

**G**

geostationary orbit (GEO) 222
global area network (GAN) 17

**H**

Hypertext Editing System (HES) 265
Hypertext Markup Language (HTML) 255
HyperText Transfer Protocol (HTTP) 260

**I**

Integrated Services Digital Network (ISDN) 87, 92
International Organization for Standardization (ISO) 174
International Telecommunication Union

(ITU) 226, 241
Internet Architecture Board (IAB) 48, 49, 50
Internet Corporation for Assigned Names and Numbers (ICANN) 47
Internet Engineering Steering Group (IESG) 48, 49, 50
Internet Engineering Task Force (IETF) 47, 48, 50
Internet Governance Forum (IGF) 50
Internet Protocol Suite (TCP/IP) 85
Internet Research Steering Group (IRSG) 49
Internet Research Task Force (IRTF) 48, 49, 50
Internet Service Providers (ISP) 23
Internet Society (ISOC) 50

**L**

local area network (LAN) 4, 14, 75, 83, 85
local area networks (LANs) 171
low Earth orbit (LEO) 222

**M**

maximum transmission unit (MTU) 92
Medium Earth orbit (MEO) 222
metropolitan area network (MAN) 85
metropolitan area networks (MANs) 171
Military Network (MILNET) 197
multistation access unit (MAU) 81

**N**

National Center for Supercomputing Applications (NCSA) 261
National Physical Laboratory (NPL) 194
National Polar-orbiting Operational Environmental Satellite System (NPOESS) 226
National Science Foundation (NSF) 192
Network Information Center (NIC) 197

**P**

Packetized Elementary Stream (PES) 71
Personal area network (PAN) 126
personal area networks (PANs) 85
program stream (PS) 72

**Q**

quality of service (QoS) 85

**R**

Request for Comments (RFCs) 49
Request for Quotation (RFQ) 195
RIPE Network Coordination Centre (RIPE NCC) 48
Robust transmission protocol 123

**S**

segmentation and reassembly (SAR) 92
semi-automatic business research environment (SABRE) 2
Semi-Automatic Ground Environment (SAGE) 2
signal-to-noise ratio (SNR) 131
Star network topology 78
start frame delimiter (SFD) 181
System Development Corporation (SDC) 194

**T**

Telecommunications 217, 252
Terminal Interface Processor (TIP) 198
Time to live (TTL) 70
top-level domains (TLDs) 47
Transmission Control Protocol (TCP) 67
Transport Layer Security (TLS) 125
transport stream (TS) 72
Tunneled Direct Link Setup (TDLS) 130

**U**

Uniform Resource Locators (URLs) 255
universal document identifier (UDI) 265
University of Illinois at Urbana-Champaign (UIUC) 261
unshielded twisted-pair cables (UTP) 178

**V**

Virtual Channel Identifier (VCI) 93
virtual private network (VPN) 16

## W

wide area networks (WANs) 16
wide area network (WAN) 2, 15, 16, 83, 85, 109
Wi-Fi Protected Setup (WPS) 125
wireless local area network (WLAN) 126, 127
World Wide Web (\ 258
World Wide Web Consortium (W3C) 262, 266

# Computer Networking Essentials

Computer networking refers to the study and analysis of the communication process among various computing devices or computer systems that are linked or networked, together to exchange information and share resources. Computer networking depends on the theoretical application and practical implementation of fields like computer engineering, computer sciences, information technology and telecommunication. Today the world scenario is changing. Data Communication and network have changed the way business and other daily affair works. Now, they rely on computer networks and internetwork. A set of devices often mentioned as nodes connected by media link is called a Network. A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called Communication channels. Computer network is a telecommunication channel through which we can share our data. It is also called data network. The best example of a computer network is the Internet. Computer network does not mean a system with control unit and other systems as its slave. It is called a distributed system. Computer networks can be broken down historically into topologies, which is a technique of connecting computers. The most common topology today is a collapsed ring. This is due to the success of a network protocol called the Ethernet. This protocol, or a network language, supports the Internet, Local Area Networks, and Wide Area Networks. A router, network card and protocols are the essential pillars upon which any network is built. Computer networks are the backbone of modern-day communication. Even public switched telephone networks are controlled by computer systems; most telephonic services are also working with IP. The increasing scope of communication has led to much advancement in the networking field and in its relative industries like hardware, software manufacturing and integration.



Charlemagne acquired his Bachelor's degree at the University of Caloocan City in 2012, He is an IT enthusiast that focuses on real-world innovations using information systems in multiple platforms. He is the current CEO for Carlo Solutions a Philippine based company that delivers Sales and Marketing improvement through the use of information systems.

Delve Publishing

ISBN 978-1-68095-671-9