# Network Engineering

Shameka Deal

First Edition, 2012

ISBN 978-81-323-3088-2



*Published by:*
**Research World**
4735/22 Prakashdeep Bldg,
Ansari Road, Darya Ganj,
Delhi - 110002
Email: info@wtbooks.com

# Table of Contents

**Chapter 1**

# Computer Network

A **computer network**, often simply referred to as a network, is a collection of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources. Networks may be classified according to a wide variety of characteristics. A computer network allows sharing of resources and information among interconnected devices.

## *History*

Early networks of communicating computers included the military radar system Semi-Automatic Ground Environment (SAGE) and its relative the commercial airline reservation system Semi-Automatic Business Research Environment (SABRE), started in the late 1950s. In the 1960s, the Advanced Research Projects Agency (ARPA) started funding the design of the Advanced Research Projects Agency Network (ARPANET) for the United States Department of Defense. Development of the network began in 1969, based on designs developed during the 1960s. The ARPANET evolved into the modern Internet.

## *Purpose*

Computer networks can be used for a variety of purposes:

- *Facilitating communications.* Using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing.
- *Sharing hardware.* In a networked environment, each computer on a network may access and use hardware resources on the network, such as printing a document on a shared network printer.
- *Sharing files, data, and information.* In a network environment, authorized user may access data and information stored on other computers on the network. The capability of providing access to data and information on shared storage devices is an important feature of many networks.

- *Sharing software.* Users connected to a network may run application programs on remote computers.
- *Information preservation.*
- *Easy communication*

## *Network classification*

The following list presents categories used for classifying networks.

### Connection method

Computer networks can be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as optical fiber, Ethernet, wireless LAN, HomePNA, power line communication or G.hn.

Ethernet as it is defined by IEEE 802 utilizes various standards and mediums that enable communication between devices. Frequently deployed devices include hubs, switches, bridges, or routers. Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium. 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.

### Wired technologies

- *Twisted pair wire* is the most widely used medium for 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 networking cabling consist 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 100 million bits per second. Twisted pair cabling comes in two forms which are Unshielded Twisted Pair (UTP) and Shielded twisted-pair (STP) which are rated in categories which are manufactured in different increments for various scenarios.

- *Coaxial cable* is widely used for cable television systems, office buildings, and other work-sites for local area networks. The cables consist of copper or aluminum wire wrapped with insulating layer typically of a flexible material with a high dielectric constant, all of which are surrounded by a conductive layer. The layers of insulation help minimize interference and distortion. Transmission speed range from 200 million to more than 500 million bits per second.

- *Optical fiber cable* consists of one or more filaments of glass fiber wrapped in protective layers that carries a data by means of pulses of light. It transmits light which can travel over extended distances. Fiber-optic cables are not affected by electromagnetic radiation. Transmission speed may reach trillions of bits per

second. The transmission speed of fiber optics is hundreds of times faster than for coaxial cables and thousands of times faster than a twisted-pair wire.A recent innovation in fiber-optic cable is the use of colored light.Instead of carrying one message in a stream of white light impulses, this technology can carry multiple signals in a single strand.

## Wireless technologies

- *Terrestrial microwave* – Terrestrial microwaves use Earth-based transmitter and receiver. The equipment looks similar to satellite dishes. Terrestrial microwaves use low-gigahertz range, which limits all communications to line-of-sight. Path between relay stations spaced approx, 30 miles apart. Microwave antennas are usually placed on top of buildings, towers, hills, and mountain peaks.

- *Communications satellites* – The satellites use microwave radio as their telecommunications medium which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically 22,000 miles (for geosynchronous satellites) 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 are divided to different geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.

- *Wireless LANs* – Wireless local area network use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. An example of open-standards wireless radio-wave technology is IEEE.

- Infrared communication , which can transmit signals between devices within small distances not more than 10 meters peer to peer or ( face to face ) without any body in the line of transmitting.

## Scale

Networks are often classified as local area network (LAN), wide area network (WAN), metropolitan area network (MAN), personal area network (PAN), virtual private network (VPN), campus area network (CAN), storage area network (SAN), and others, depending on their scale, scope and purpose, e.g., controller area network (CAN) usage, trust level, and access right often differ between these types of networks. LANs tend to be designed for internal use by an organization's internal systems and employees in individual physical locations, such as a building, while WANs may connect physically separate parts of an organization and may include connections to third parties.

## Functional relationship (network architecture)

Computer networks may be classified according to the functional relationships which exist among the elements of the network, e.g., active networking, client–server, Wireless ad hoc network and peer-to-peer (workgroup) architecture.

## Network topology

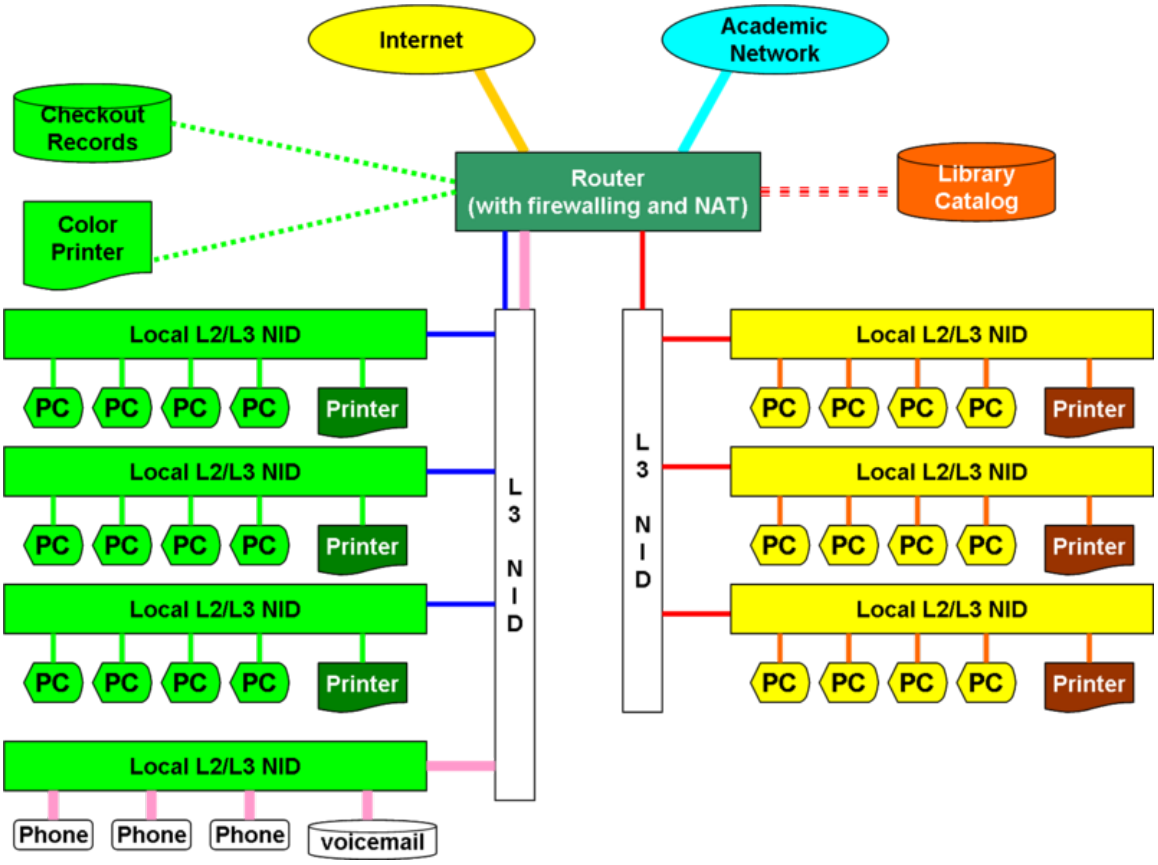
Computer networks may be classified according to the network topology upon which the network is based, such as bus network, star network, ring network, mesh network. Network topology is the coordination by which devices in the network are arranged in their logical relations to one another, independent of physical arrangement. Even if networked computers are physically placed in a linear arrangement and are connected to a hub, the network has a star topology, rather than a bus topology. In this regard the visual and operational characteristics of a network are distinct. Networks may be classified based on the method of data used to convey the data, these include digital and analog networks.

# *Types of networks based on physical scope*

Common types of computer networks may be identified by their scale.

## Local area network

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




Typical library network, in a branching tree topology and controlled access to resources

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

The defining characteristics of LANs, in contrast to WANs (Wide Area Networks), include their higher data transfer rates, smaller geographic range, and no need for leased telecommunication lines. Current Ethernet or other IEEE 802.3 LAN technologies operate at speeds up to 10 Gbit/s. This is the data transfer rate. IEEE has projects investigating the standardization of 40 and 100 Gbit/s.

## 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.

## Home area network

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

## Wide area network

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

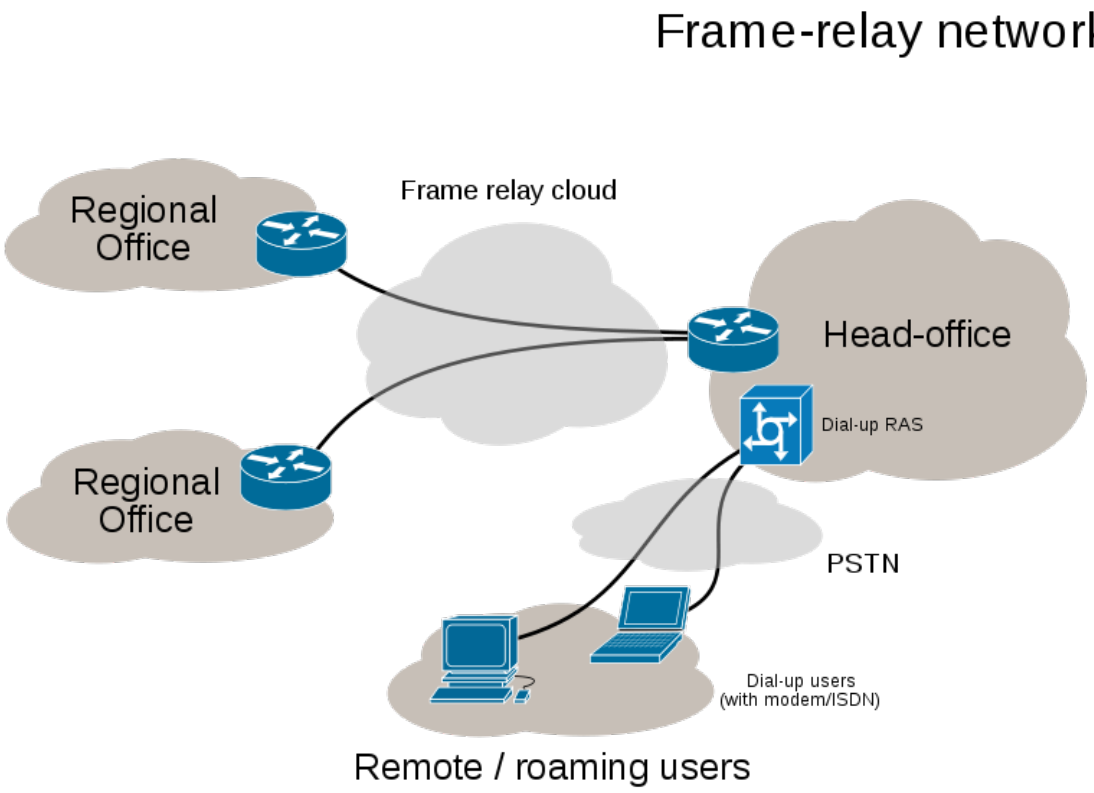
## Campus network

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

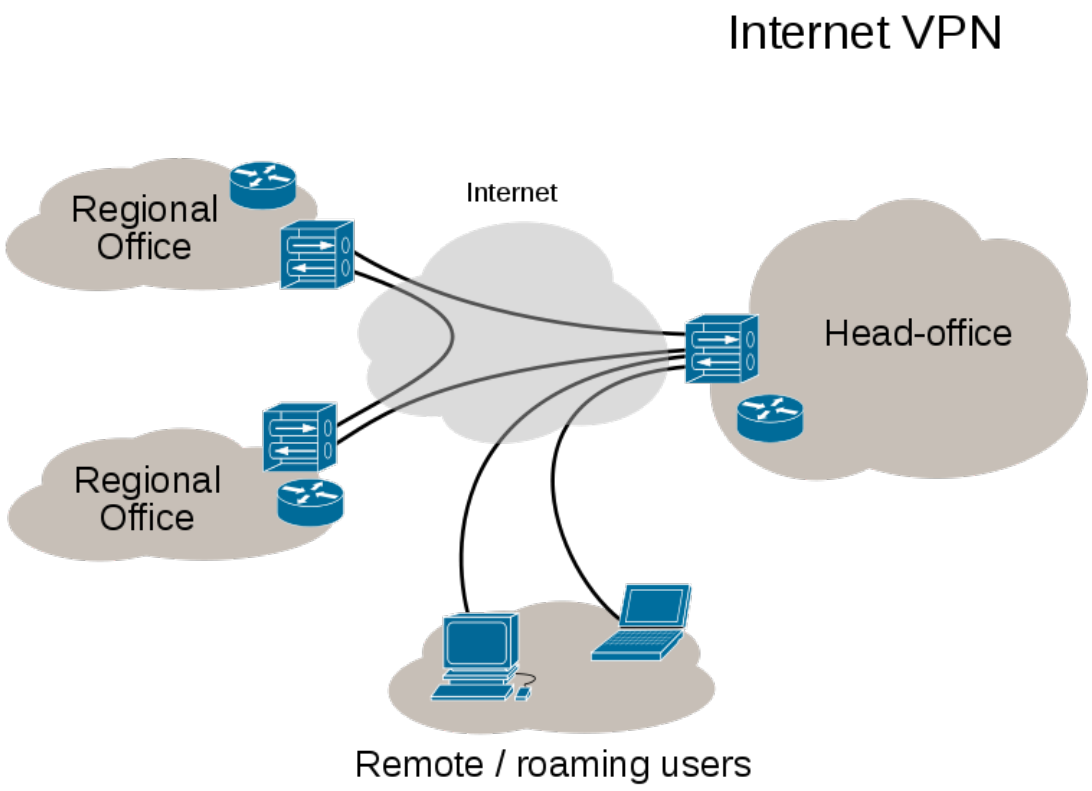
In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including; academic departments, the university library and student residence halls.

## Metropolitan area network

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




Sample EPN made of Frame relay WAN connections and dialup remote access.




Sample VPN used to interconnect 3 offices and remote users

## Enterprise private network

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

## Virtual private network

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

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

## Internetwork

An internetwork is the connection of two or more private computer networks via a common routing technology (OSI Layer 3) using routers. The Internet is an aggregation of many internetworks, hence its name was shortened to Internet.

## Backbone network

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

A large corporation that has many locations may have a backbone network that ties all of the locations together, for example, if a server cluster needs to be accessed by different departments of a company that are located at different geographical locations. The pieces of the network connections (for example: ethernet, wireless) that bring these departments together is often mentioned as network backbone. Network congestion is often taken into consideration while designing backbones.

Backbone networks should not be confused with the Internet backbone.

## Global area network

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

## Internet

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

Participants in the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet Protocol Suite and an addressing system (IP addresses) administered by the Internet Assigned Numbers Authority and address registries. Service providers and large enterprises

exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

## Intranets and extranets

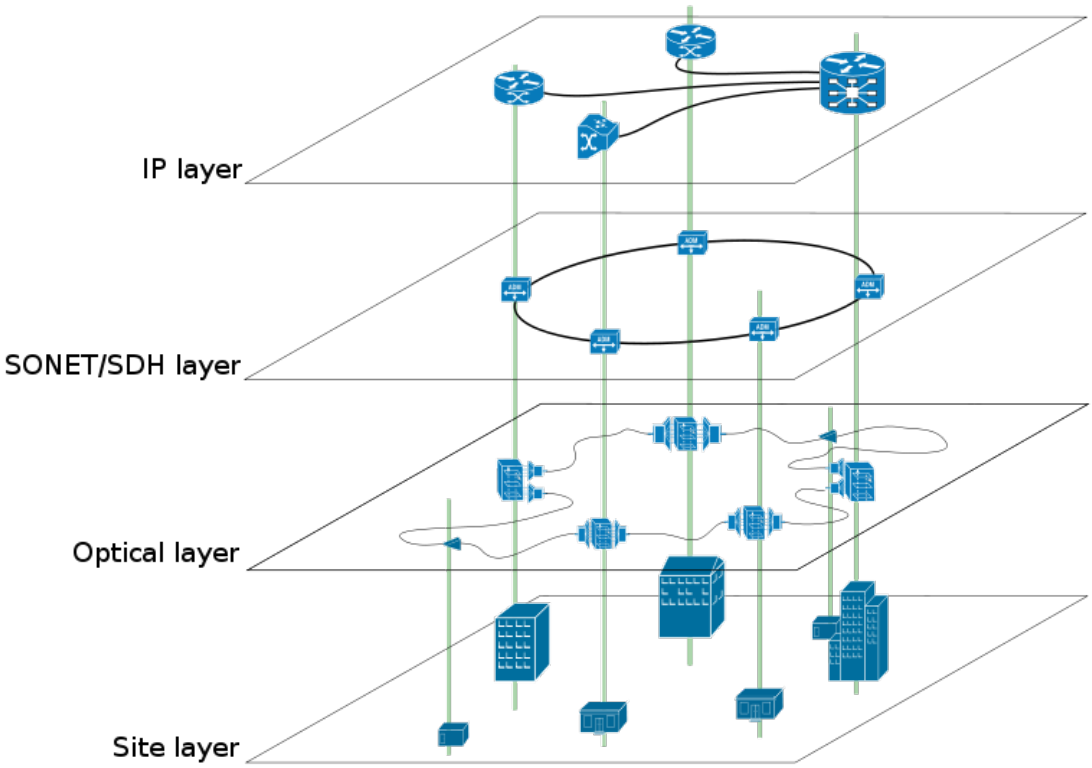
Intranets and extranets are parts or extensions of a computer network, usually a local area network.

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

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

## Overlay network

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay are connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network.




A sample overlay network: IP over SONET over Optical

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

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

Nowadays the Internet is the basis for many overlaid networks that can be constructed to permit routing of messages to destinations specified by an IP address. For example, distributed hash tables can be used to route messages to a node having a specific logical address, whose IP address is known in advance.

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

nodes, but it can control, for example, the sequence of overlay nodes a message traverses before reaching its destination.

For example, Akamai Technologies manages an overlay network that provides reliable, efficient content delivery (a kind of multicast). Academic research includes End System Multicast and Overcast for multicast; RON (Resilient Overlay Network) for resilient routing; and OverQoS for quality of service guarantees, among others. A backbone network or network backbone is a part of computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than the networks connected to it.

## *Basic hardware components*

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

### Network interface cards

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

Each network interface card has its unique id. This is written on a chip which is mounted on the card.

### Repeaters

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

## Bridges

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

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

Bridges come in three basic types:

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

## Switches

A network switch is a device that forwards and filters OSI layer 2 datagrams (chunks of data communication) between ports (connected cables) based on the MAC addresses in the packets. A switch is distinct from a hub in that it only forwards the frames to the ports involved in the communication rather than all ports connected. A switch breaks the collision domain but represents itself as a broadcast domain. Switches make forwarding decisions of frames on the basis of MAC addresses. A switch normally has numerous ports, facilitating a star topology for devices, and cascading additional switches.[1] Some switches are capable of routing based on Layer 3 addressing or additional logical levels; these are called multi-layer switches. The term *switch* is used loosely in marketing to encompass devices including routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier).

## Routers

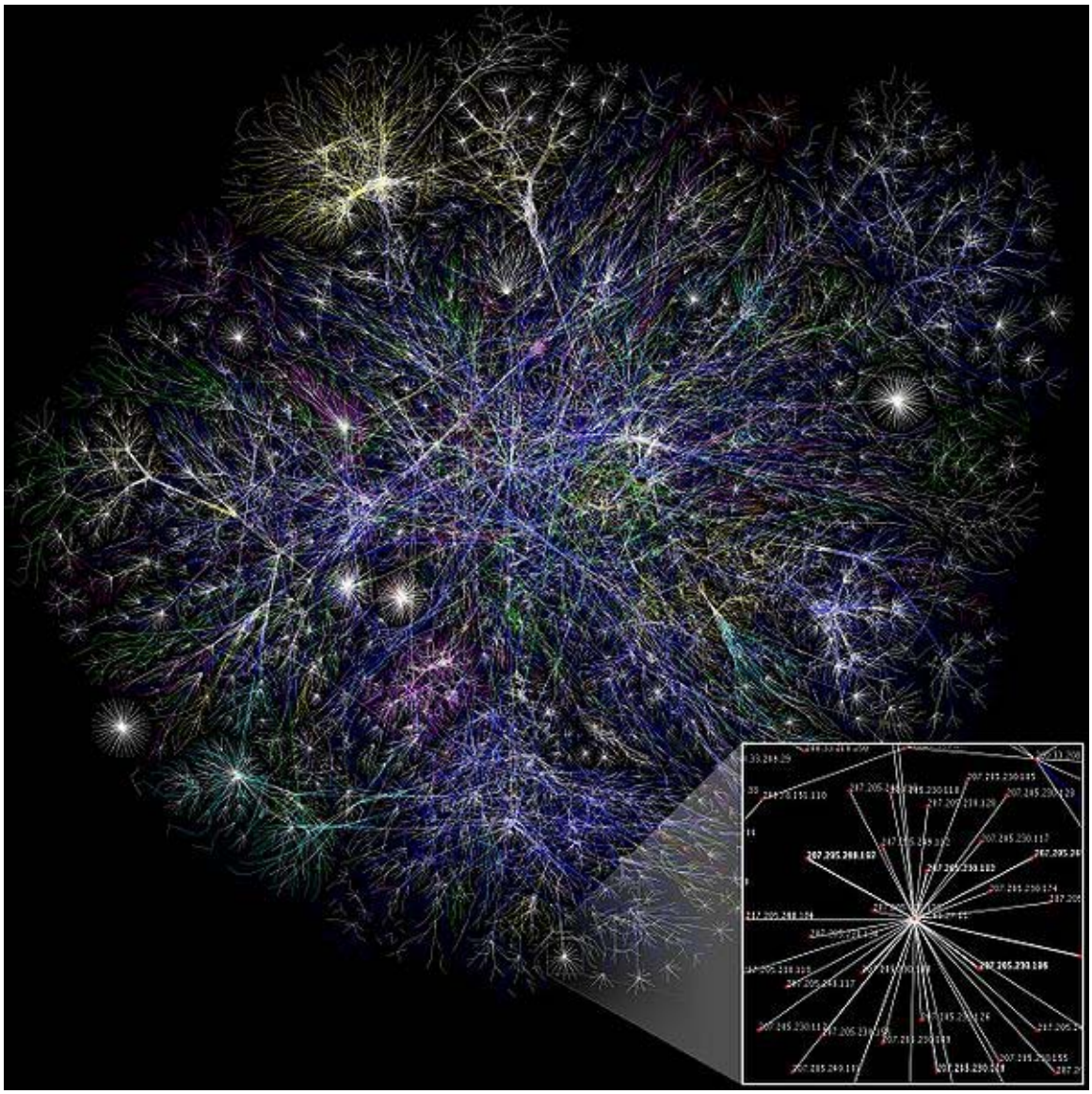
A router is an internetworking device that forwards packets between networks by processing information found in the datagram or packet (Internet protocol information from Layer 3 of the OSI Model). In many situations, this information is processed in conjunction with the routing table (also known as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

## Firewalls

Firewalls are the most important aspect of a network with respect to security. A firewalled system does not need every interaction or data transfer monitored by a human, as automated processes can be set up to assist in rejecting access requests from unsafe sources, and allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in 'cyber' attacks for the purpose of stealing/corrupting data, planting viruses, etc.

Chapter 2

# Internet



Visualization from the Opte Project of the various routes through a portion of the Internet

The **Internet** is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a *network of networks* that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail.

Most traditional communications media including telephone, music, film, and television are reshaped or redefined by the Internet, giving birth to new services such as Voice over Internet Protocol (VoIP) and IPTV. Newspaper, book and other print publishing are adapting to Web site technology, or are reshaped into blogging and web feeds. The Internet has enabled or accelerated new forms of human interactions through instant messaging, Internet forums, and social networking. Online shopping has boomed both for major retail outlets and small artisans and traders. Business-to-business and financial services on the Internet affect supply chains across entire industries.

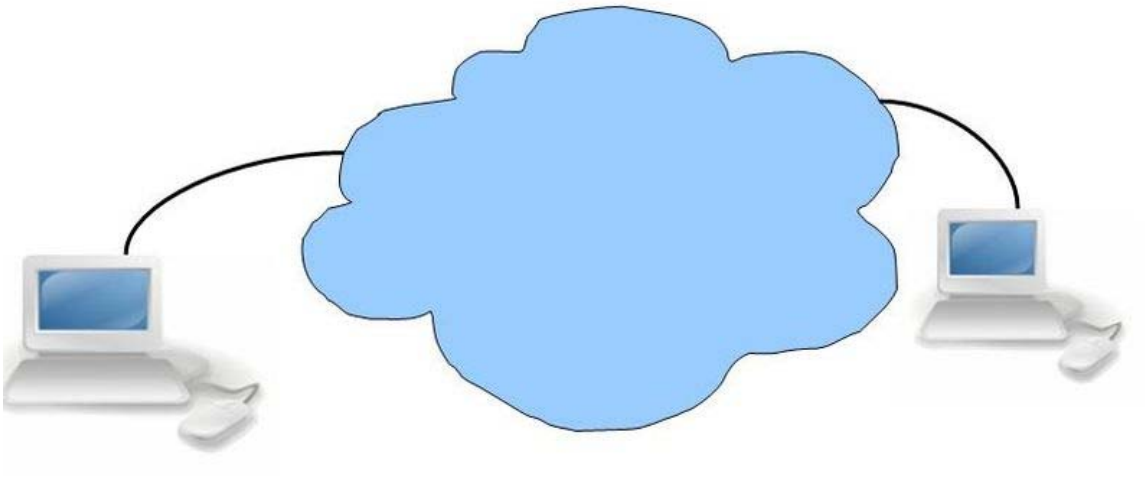
The origins of the Internet reach back to research of the 1960s, commissioned by the United States government in collaboration with private commercial interests to build robust, fault-tolerant, and distributed computer networks. The funding of a new U.S. backbone by the National Science Foundation in the 1980s, as well as private funding for other commercial backbones, led to worldwide participation in the development of new networking technologies, and the merger of many networks. The commercialization of what was by the 1990s an international network resulted in its popularization and incorporation into virtually every aspect of modern human life. As of 2009, an estimated quarter of Earth's population used the services of the Internet.

The Internet has no centralized governance in either technological implementation or policies for access and usage; each constituent network sets its own standards. Only the overreaching definitions of the two principal name spaces in the Internet, the Internet Protocol address space and the Domain Name System, are directed by a maintainer organization, the Internet Corporation for Assigned Names and Numbers (ICANN). The technical underpinning and standardization of the core protocols (IPv4 and IPv6) is an activity of the Internet Engineering Task Force (IETF), a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise.

## *Terminology*

*Internet* is a short form of the technical term internetwork, the result of interconnecting computer networks with special gateways or routers. The Internet is also often referred to as *the Net*.

The term *the Internet*, when referring to the entire global system of IP networks, has been treated as a proper noun and written with an initial capital letter. Some guides specify that the word should be capitalized as a noun but not capitalized as an adjective.



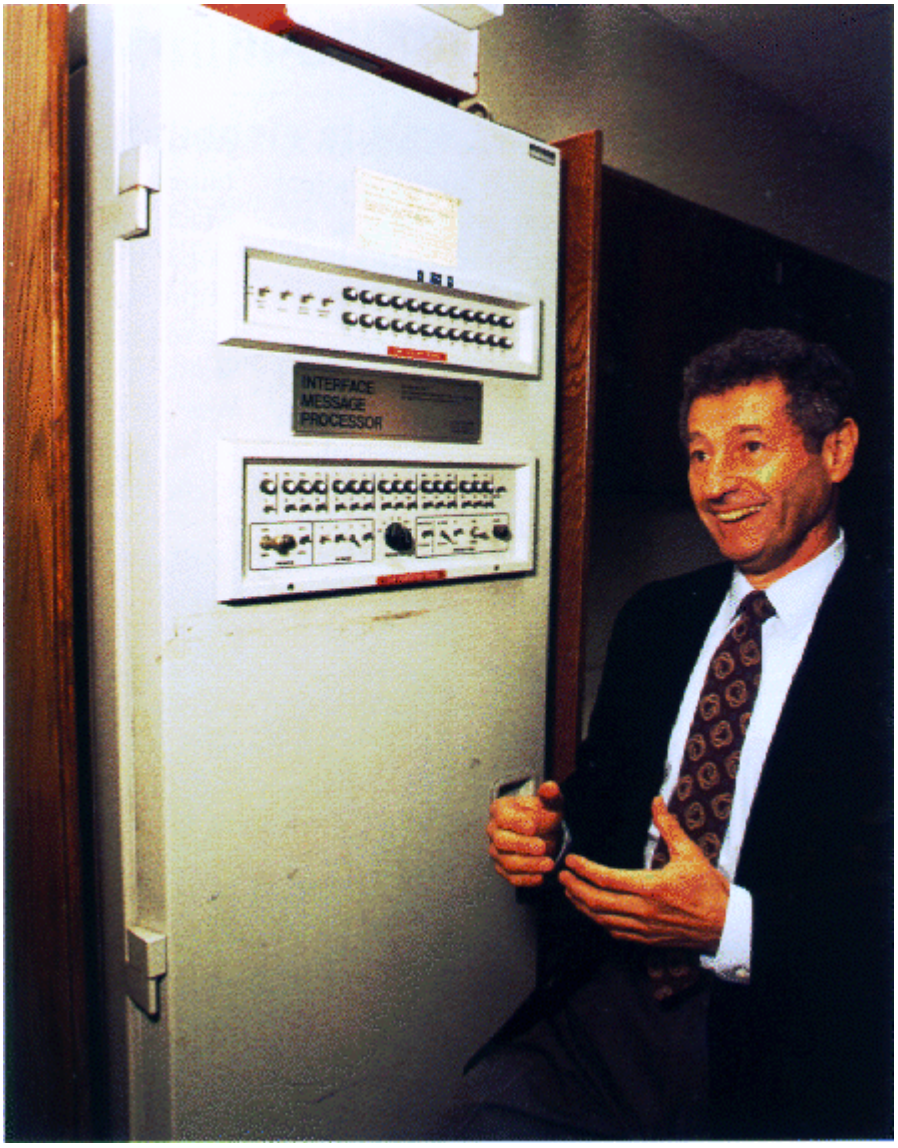
Depiction of the Internet as a *cloud* in network diagrams

The terms *Internet* and *World Wide Web* are often used in everyday speech without much distinction. However, the Internet and the World Wide Web are not one and the same. The Internet is a global data communications system. It is a hardware and software infrastructure that provides connectivity between computers. In contrast, the Web is one of the services communicated via the Internet. It is a collection of interconnected documents and other resources, linked by hyperlinks and URLs.

In many technical illustrations when the precise location or interrelation of Internet resources is not important, extended networks such as the Internet are often depicted as a cloud. The verbal image has been formalized in the newer concept of cloud computing.

## *History*

The USSR's launch of Sputnik spurred the United States to create the Advanced Research Projects Agency (ARPA or DARPA) in February 1958 to regain a technological lead. ARPA created the Information Processing Technology Office (IPTO) to further the research of the Semi Automatic Ground Environment (SAGE) program, which had networked country-wide radar systems together for the first time. The IPTO's purpose was to find ways to address the US military's concern about survivability of their communications networks, and as a first step interconnect their computers at the Pentagon, Cheyenne Mountain, and Strategic Air Command headquarters (SAC). J. C. R. Licklider, a promoter of universal networking, was selected to head the IPTO. Licklider moved from the Psycho-Acoustic Laboratory at Harvard University to MIT in 1950, after becoming interested in information technology. At MIT, he served on a committee that established Lincoln Laboratory and worked on the SAGE project. In 1957 he became a Vice President at BBN, where he bought the first production PDP-1 computer and conducted the first public demonstration of time-sharing.




Professor Leonard Kleinrock with the first ARPANET Interface Message Processors at UCLA


A plaque commemorating the birth of the Internet at Stanford University

At the IPTO, Licklider's successor Ivan Sutherland in 1965 got Lawrence Roberts to start a project to make a network, and Roberts based the technology on the work of Paul Baran, who had written an exhaustive study for the United States Air Force that recommended packet switching (opposed to circuit switching) to achieve better network robustness and disaster survivability. Roberts had worked at the MIT Lincoln Laboratory originally established to work on the design of the SAGE system. UCLA professor Leonard Kleinrock had provided the theoretical foundations for packet networks in 1962, and later, in the 1970s, for hierarchical routing, concepts which have been the underpinning of the development towards today's Internet.

Sutherland's successor Robert Taylor convinced Roberts to build on his early packet switching successes and come and be the IPTO Chief Scientist. Once there, Roberts prepared a report called *Resource Sharing Computer Networks* which was approved by Taylor in June 1968 and laid the foundation for the launch of the working ARPANET the following year.

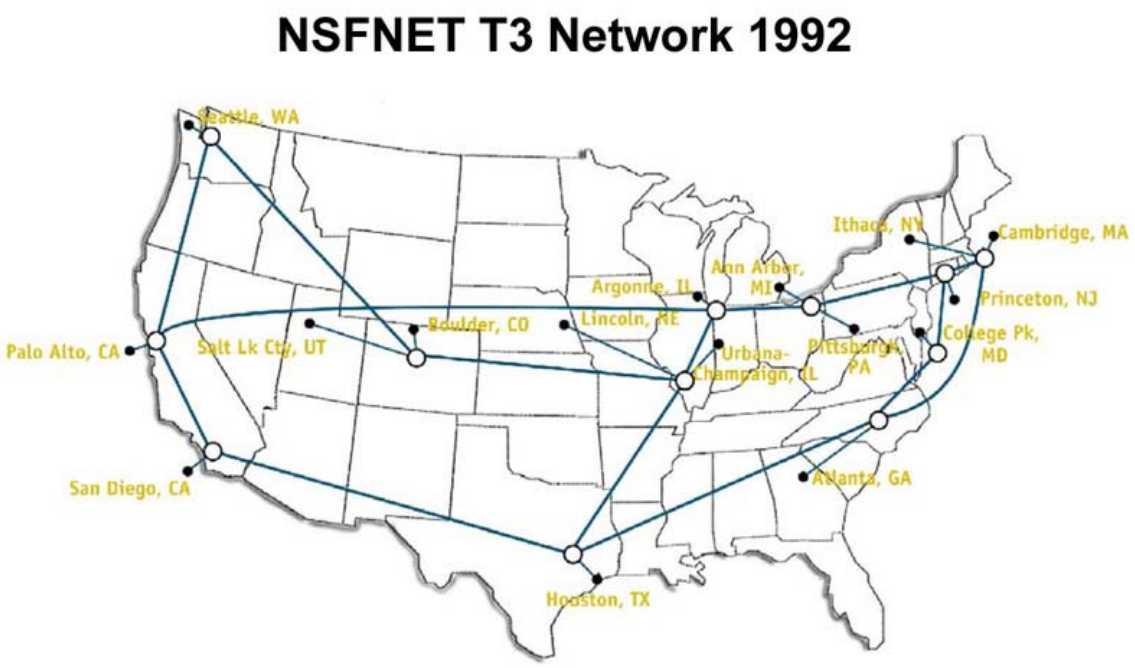
After much work, the first two nodes of what would become the ARPANET were interconnected between Kleinrock's Network Measurement Center at the UCLA's School of Engineering and Applied Science and Douglas Engelbart's NLS system at SRI International (SRI) in Menlo Park, California, on 29 October 1969. The third site on the ARPANET was the Culler-Fried Interactive Mathematics center at the University of California at Santa Barbara, and the fourth was the University of Utah Graphics Department. In an early sign of future growth, there were already fifteen sites connected to the young ARPANET by the end of 1971.

In an independent development, Donald Davies at the UK National Physical Laboratory developed the concept of packet switching in the early 1960s, first giving a talk on the subject in 1965, after which the teams in the new field from two sides of the Atlantic ocean first became acquainted. It was actually Davies' coinage of the wording *packet* and *packet switching* that was adopted as the standard terminology. Davies also built a packet-switched network in the UK, called the Mark I in 1970. Bolt, Beranek & Newman

(BBN), the private contractors for ARPANET, set out to create a separate commercial version after establishing "value added carriers" was legalized in the U.S. The network they established was called Telenet and began operation in 1975, installing free public dial-up access in cities throughout the U.S. Telenet was the first packet-switching network open to the general public.

Following the demonstration that packet switching worked on the ARPANET, the British Post Office, Telenet, DATAPAC and TRANSPAC collaborated to create the first international packet-switched network service. In the UK, this was referred to as the International Packet Switched Service (IPSS), in 1978. The collection of X.25-based networks grew from Europe and the US to cover Canada, Hong Kong and Australia by 1981. The X.25 packet switching standard was developed in the CCITT (now called ITU-T) around 1976. X.25 was independent of the TCP/IP protocols that arose from the experimental work of DARPA on the ARPANET, Packet Radio Net, and Packet Satellite Net during the same time period.

The early ARPANET ran on the Network Control Program (NCP), implementing the host-to-host connectivity and switching layers of the protocol stack, designed and first implemented in December 1970 by a team called the Network Working Group (NWG) led by Steve Crocker. To respond to the network's rapid growth as more and more locations connected, Vinton Cerf and Robert Kahn developed the first description of the now widely used TCP protocols during 1973 and published a paper on the subject in May 1974. Use of the term "Internet" to describe a single global TCP/IP network originated in December 1974 with the publication of RFC 675, the first full specification of TCP that was written by Vinton Cerf, Yogen Dalal and Carl Sunshine, then at Stanford University. During the next nine years, work proceeded to refine the protocols and to implement them on a wide range of operating systems. The first TCP/IP-based wide-area network was operational by 1 January 1983 when all hosts on the ARPANET were switched over from the older NCP protocols.




T3 NSFNET Backbone, c. 1992

In 1985, the United States' National Science Foundation (NSF) commissioned the construction of the NSFNET, a university 56 kilobit/second network backbone using computers called "fuzzballs" by their inventor, David L. Mills. The following year, NSF sponsored the conversion to a higher-speed 1.5 megabit/second network that became operational in 1988. A key decision to use the DARPA TCP/IP protocols was made by Dennis Jennings, then in charge of the Supercomputer program at NSF. The NSFNET backbone was upgraded to 45 Mbps in 1991 and decommissioned in 1995 when it was replaced by new backbone networks operated by commercial Internet Service Providers.

The opening of the NSFNET to other networks began in 1988.[1] The US Federal Networking Council approved the interconnection of the NSFNET to the commercial MCI Mail system in that year and the link was made in the summer of 1989. Other commercial electronic mail services were soon connected, including OnTyme, Telemail and Compuserve. In that same year, three commercial Internet service providers (ISPs) began operations: UUNET, PSINet, and CERFNET. Important, separate networks that offered gateways into, then later merged with, the Internet include Usenet and BITNET. Various other commercial and educational networks, such as Telenet (by that time renamed to Sprintnet), Tymnet, Compuserve and JANET were interconnected with the growing Internet in the 1980s as the TCP/IP protocol became increasingly popular. The adaptability of TCP/IP to existing communication networks allowed for rapid growth. The open availability of the specifications and reference code permitted commercial vendors to build interoperable network components, such as routers, making standardized network gear available from many companies. This aided in the rapid growth of the Internet and the proliferation of local-area networking. It seeded the widespread

implementation and rigorous standardization of TCP/IP on UNIX and virtually every other common operating system.


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

Although the basic applications and guidelines that make the Internet possible had existed for almost two decades, the network did not gain a public face until the 1990s. On 6 August 1991, CERN, a pan-European organization for particle research, publicized the new World Wide Web project. The Web was invented by British scientist Tim Berners-Lee in 1989. An early popular web browser was ViolaWWW, patterned after HyperCard and built using the X Window System. It was eventually replaced in popularity by the Mosaic web browser. In 1993, the National Center for Supercomputing Applications at the University of Illinois released version 1.0 of Mosaic, and by late 1994 there was growing public interest in the previously academic, technical Internet. By 1996 usage of the word *Internet* had become commonplace, and consequently, so had its use as a synecdoche in reference to the World Wide Web.

Meanwhile, over the course of the decade, the Internet successfully accommodated the majority of previously existing public computer networks (although some networks, such as FidoNet, have remained separate). During the late 1990s, it was estimated that traffic on the public Internet grew by 100 percent per year, while the mean annual growth in the

number of Internet users was thought to be between 20% and 50%. This growth is often attributed to the lack of central administration, which allows organic growth of the network, as well as the non-proprietary open nature of the Internet protocols, which encourages vendor interoperability and prevents any one company from exerting too much control over the network. The estimated population of Internet users is 1.97 billion as of 30 June 2010.

From 2009 onward, the Internet is expected to grow significantly in Brazil, Russia, India, China, and Indonesia (BRICI countries). These countries have large populations and moderate to high economic growth, but still low Internet penetration rates. In 2009, the BRICI countries represented about 45 percent of the world's population and had approximately 610 million Internet users, but by 2015, Internet users in BRICI countries will double to 1.2 billion, and will triple in Indonesia.

## *Technology*

### Protocols

The complex communications infrastructure of the Internet consists of its hardware components and a system of software layers that control various aspects of the architecture. While the hardware can often be used to support other software systems, it is the design and the rigorous standardization process of the software architecture that characterizes the Internet and provides the foundation for its scalability and success. The responsibility for the architectural design of the Internet software systems has been delegated to the Internet Engineering Task Force (IETF). The IETF conducts standard-setting work groups, open to any individual, about the various aspects of Internet architecture. Resulting discussions and final standards are published in a series of publications, each called a Request for Comments (RFC), freely available on the IETF web site. The principal methods of networking that enable the Internet are contained in specially designated RFCs that constitute the Internet Standards. Other less rigorous documents are simply informative, experimental, or historical, or document the best current practices (BCP) when implementing Internet technologies.

The Internet Standards describe a framework known as the Internet Protocol Suite. This is a model architecture that divides methods into a layered system of protocols (RFC 1122, RFC 1123). The layers correspond to the environment or scope in which their services operate. At the top is the Application Layer, the space for the application-specific networking methods used in software applications, e.g., a web browser program. Below this top layer, the Transport Layer connects applications on *different hosts* via the network (e.g., client–server model) with appropriate data exchange methods. Underlying these layers are the core networking technologies, consisting of two layers. The Internet Layer enables computers to identify and locate each other via Internet Protocol (IP) addresses, and allows them to connect to one-another via intermediate (transit) networks. Lastly, at the bottom of the architecture, is a software layer, the Link Layer, that provides connectivity between hosts on the same local network link, such as a local area network (LAN) or a dial-up connection. The model, also known as TCP/IP, is designed to be

independent of the underlying hardware which the model therefore does not concern itself with in any detail. Other models have been developed, such as the Open Systems Interconnection (OSI) model, but they are not compatible in the details of description, nor implementation, but many similarities exist and the TCP/IP protocols are usually included in the discussion of OSI networking.

The most prominent component of the Internet model is the Internet Protocol (IP) which provides addressing systems (IP addresses) for computers on the Internet. IP enables internetworking and essentially establishes the Internet itself. IP Version 4 (IPv4) is the initial version used on the first generation of the today's Internet and is still in dominant use. It was designed to address up to ~4.3 billion ($10^9$) Internet hosts. However, the explosive growth of the Internet has led to IPv4 address exhaustion which is estimated to enter its final stage in approximately 2011. A new protocol version, IPv6, was developed in the mid 1990s which provides vastly larger addressing capabilities and more efficient routing of Internet traffic. IPv6 is currently in commercial deployment phase around the world and Internet address registries (RIRs) have begun to urge all resource managers to plan rapid adoption and conversion.

IPv6 is not interoperable with IPv4. It essentially establishes a "parallel" version of the Internet not directly accessible with IPv4 software. This means software upgrades or translator facilities are necessary for every networking device that needs to communicate on the IPv6 Internet. Most modern computer operating systems are already converted to operate with both versions of the Internet Protocol. Network infrastructures, however, are still lagging in this development. Aside from the complex physical connections that make up its infrastructure, the Internet is facilitated by bi- or multi-lateral commercial contracts (e.g., peering agreements), and by technical specifications or protocols that describe how to exchange data over the network. Indeed, the Internet is defined by its interconnections and routing policies.

## Structure

The Internet structure and its usage characteristics have been studied extensively. It has been determined that both the Internet IP routing structure and hypertext links of the World Wide Web are examples of scale-free networks. Similar to the way the commercial Internet providers connect via Internet exchange points, research networks tend to interconnect into large subnetworks such as GEANT, GLORIAD, Internet2 (successor of the Abilene Network), and the UK's national research and education network JANET. These in turn are built around smaller networks.

Many computer scientists describe the Internet as a "prime example of a large-scale, highly engineered, yet highly complex system". The Internet is extremely heterogeneous; for instance, data transfer rates and physical characteristics of connections vary widely. The Internet exhibits "emergent phenomena" that depend on its large-scale organization. For example, data transfer rates exhibit temporal self-similarity. The principles of the routing and addressing methods for traffic in the Internet reach back to their origins the

1960s when the eventual scale and popularity of the network could not be anticipated. Thus, the possibility of developing alternative structures is investigated.

## *Governance*


ICANN headquarters in Marina Del Rey, California, United States

The Internet is a globally distributed network comprising many voluntarily interconnected autonomous networks. It operates without a central governing body. However, to maintain interoperability, all technical and policy aspects of the underlying core infrastructure and the principal name spaces are administered by the Internet Corporation for Assigned Names and Numbers (ICANN), headquartered in Marina del Rey, California. ICANN is the authority that coordinates the assignment of unique identifiers for use on the Internet, including domain names, Internet Protocol (IP) addresses, application port numbers in the transport protocols, and many other parameters. Globally unified name spaces, in which names and numbers are uniquely assigned, are essential for the global reach of the Internet. ICANN is governed by an international board of directors drawn from across the Internet technical, business, academic, and other non-commercial communities. The government of the United States continues to have the primary role in approving changes to the DNS root zone that lies at the heart of the domain name system. ICANN's role in coordinating the assignment of unique identifiers distinguishes it as perhaps the only central coordinating body on the

global Internet. On 16 November 2005, the World Summit on the Information Society, held in Tunis, established the Internet Governance Forum (IGF) to discuss Internet-related issues.

## *Modern uses*

The Internet is allowing greater flexibility in working hours and location, especially with the spread of unmetered high-speed connections and web applications.

The Internet can now be accessed almost anywhere by numerous means, especially through mobile Internet devices. Mobile phones, datacards, handheld game consoles and cellular routers allow users to connect to the Internet from anywhere there is a wireless network supporting that device's technology. Within the limitations imposed by small screens and other limited facilities of such pocket-sized devices, services of the Internet, including email and the web, may be available. Service providers may restrict the services offered and wireless data transmission charges may be significantly higher than other access methods.

Educational material at all levels from pre-school to post-doctoral is available from websites. Examples range from CBeebies, through school and high-school revision guides, virtual universities, to access to top-end scholarly literature through the likes of Google Scholar. In distance education, help with homework and other assignments, self-guided learning, whiling away spare time, or just looking up more detail on an interesting fact, it has never been easier for people to access educational information at any level from anywhere. The Internet in general and the World Wide Web in particular are important enablers of both formal and informal education.

The low cost and nearly instantaneous sharing of ideas, knowledge, and skills has made collaborative work dramatically easier, with the help of collaborative software. Not only can a group cheaply communicate and share ideas, but the wide reach of the Internet allows such groups to easily form in the first place. An example of this is the free software movement, which has produced, among other programs, Linux, Mozilla Firefox, and OpenOffice.org. Internet "chat", whether in the form of IRC chat rooms or channels, or via instant messaging systems, allow colleagues to stay in touch in a very convenient way when working at their computers during the day. Messages can be exchanged even more quickly and conveniently than via email. Extensions to these systems may allow files to be exchanged, "whiteboard" drawings to be shared or voice and video contact between team members.

Version control systems allow collaborating teams to work on shared sets of documents without either accidentally overwriting each other's work or having members wait until they get "sent" documents to be able to make their contributions. Business and project teams can share calendars as well as documents and other information. Such collaboration occurs in a wide variety of areas including scientific research, software development, conference planning, political activism and creative writing. Social and political collaboration is also becoming more widespread as both Internet access and

computer literacy grow. From the flash mob 'events' of the early 2000s to the use of social networking in the 2009 Iranian election protests, the Internet allows people to work together more effectively and in many more ways than was possible without it.

The Internet allows computer users to remotely access other computers and information stores easily, wherever they may be across the world. They may do this with or without the use of security, authentication and encryption technologies, depending on the requirements. This is encouraging new ways of working from home, collaboration and information sharing in many industries. An accountant sitting at home can audit the books of a company based in another country, on a server situated in a third country that is remotely maintained by IT specialists in a fourth. These accounts could have been created by home-working bookkeepers, in other remote locations, based on information emailed to them from offices all over the world. Some of these things were possible before the widespread use of the Internet, but the cost of private leased lines would have made many of them infeasible in practice. An office worker away from their desk, perhaps on the other side of the world on a business trip or a holiday, can open a remote desktop session into his normal office PC using a secure Virtual Private Network (VPN) connection via the Internet. This gives the worker complete access to all of his or her normal files and data, including email and other applications, while away from the office. This concept has been referred to among system administrators as the Virtual Private Nightmare, because it extends the secure perimeter of a corporate network into its employees' homes.

## *Services*

### Information

Many people use the terms *Internet* and *World Wide Web*, or just the *Web*, interchangeably, but the two terms are not synonymous. The World Wide Web is a global set of documents, images and other resources, logically interrelated by hyperlinks and referenced with Uniform Resource Identifiers (URIs). URIs allow providers to symbolically identify services and clients to locate and address web servers, file servers, and other databases that store documents and provide resources and access them using the Hypertext Transfer Protocol (HTTP), the primary carrier protocol of the Web. HTTP is only one of the hundreds of communication protocols used on the Internet. Web services may also use HTTP to allow software systems to communicate in order to share and exchange business logic and data.

World Wide Web browser software, such as Microsoft's Internet Explorer, Mozilla Firefox, Opera, Apple's Safari, and Google Chrome, let users navigate from one web page to another via hyperlinks embedded in the documents. These documents may also contain any combination of computer data, including graphics, sounds, text, video, multimedia and interactive content including games, office applications and scientific demonstrations. Through keyword-driven Internet research using search engines like Yahoo! and Google, users worldwide have easy, instant access to a vast and diverse

amount of online information. Compared to printed encyclopedias and traditional libraries, the World Wide Web has enabled the decentralization of information.

The Web has also enabled individuals and organizations to publish ideas and information to a potentially large audience online at greatly reduced expense and time delay. Publishing a web page, a blog, or building a website involves little initial cost and many cost-free services are available. Publishing and maintaining large, professional web sites with attractive, diverse and up-to-date information is still a difficult and expensive proposition, however. Many individuals and some companies and groups use *web logs* or blogs, which are largely used as easily updatable online diaries. Some commercial organizations encourage staff to communicate advice in their areas of specialization in the hope that visitors will be impressed by the expert knowledge and free information, and be attracted to the corporation as a result. One example of this practice is Microsoft, whose product developers publish their personal blogs in order to pique the public's interest in their work. Collections of personal web pages published by large service providers remain popular, and have become increasingly sophisticated. Whereas operations such as Angelfire and GeoCities have existed since the early days of the Web, newer offerings from, for example, Facebook and MySpace currently have large followings. These operations often brand themselves as social network services rather than simply as web page hosts.

Advertising on popular web pages can be lucrative, and e-commerce or the sale of products and services directly via the Web continues to grow.

When the Web began in the 1990s, a typical web page was stored in completed form on a web server, formatted with HTML, ready to be sent to a user's browser in response to a request. Over time, the process of creating and serving web pages has become more automated and more dynamic. Websites are often created using content management or software with, initially, very little content. Contributors to these systems, who may be paid staff, members of a club or other organization or members of the public, fill underlying databases with content using editing pages designed for that purpose, while casual visitors view and read this content in its final HTML form. There may or may not be editorial, approval and security systems built into the process of taking newly entered content and making it available to the target visitors.

## Communication

Electronic mail, or email, is an important communications service available on the Internet. The concept of sending electronic text messages between parties in a way analogous to mailing letters or memos predates the creation of the Internet. Pictures, documents and other files are sent as email attachments. Emails can be cc-ed to multiple email addresses.

Internet telephony is another common communications service made possible by the creation of the Internet. VoIP stands for Voice-over-Internet Protocol, referring to the protocol that underlies all Internet communication. The idea began in the early 1990s

with walkie-talkie-like voice applications for personal computers. In recent years many VoIP systems have become as easy to use and as convenient as a normal telephone. The benefit is that, as the Internet carries the voice traffic, VoIP can be free or cost much less than a traditional telephone call, especially over long distances and especially for those with always-on Internet connections such as cable or ADSL. VoIP is maturing into a competitive alternative to traditional telephone service. Interoperability between different providers has improved and the ability to call or receive a call from a traditional telephone is available. Simple, inexpensive VoIP network adapters are available that eliminate the need for a personal computer.

Voice quality can still vary from call to call but is often equal to and can even exceed that of traditional calls. Remaining problems for VoIP include emergency telephone number dialing and reliability. Currently, a few VoIP providers provide an emergency service, but it is not universally available. Traditional phones are line-powered and operate during a power failure; VoIP does not do so without a backup power source for the phone equipment and the Internet access devices. VoIP has also become increasingly popular for gaming applications, as a form of communication between players. Popular VoIP clients for gaming include Ventrilo and Teamspeak. Wii, PlayStation 3, and Xbox 360 also offer VoIP chat features.

## Data transfer

File sharing is an example of transferring large amounts of data across the Internet. A computer file can be emailed to customers, colleagues and friends as an attachment. It can be uploaded to a website or FTP server for easy download by others. It can be put into a "shared location" or onto a file server for instant use by colleagues. The load of bulk downloads to many users can be eased by the use of "mirror" servers or peer-to-peer networks. In any of these cases, access to the file may be controlled by user authentication, the transit of the file over the Internet may be obscured by encryption, and money may change hands for access to the file. The price can be paid by the remote charging of funds from, for example, a credit card whose details are also passed—usually fully encrypted—across the Internet. The origin and authenticity of the file received may be checked by digital signatures or by MD5 or other message digests. These simple features of the Internet, over a worldwide basis, are changing the production, sale, and distribution of anything that can be reduced to a computer file for transmission. This includes all manner of print publications, software products, news, music, film, video, photography, graphics and the other arts. This in turn has caused seismic shifts in each of the existing industries that previously controlled the production and distribution of these products.

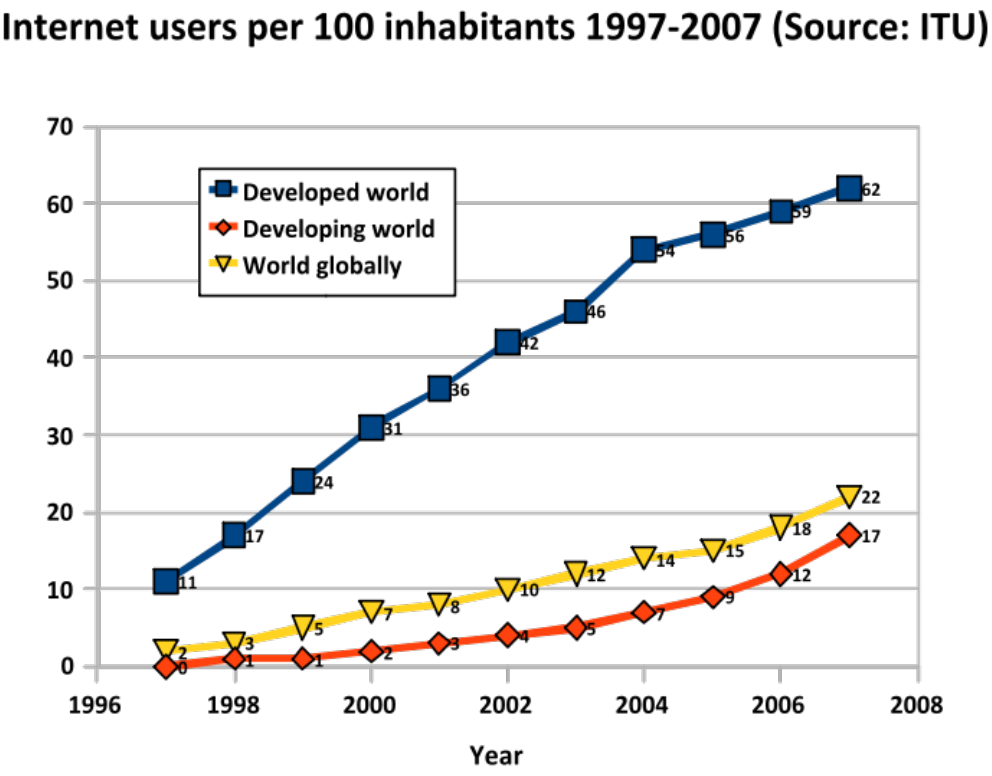
Streaming media is the real-time delivery of digital media for the immediate consumption or enjoyment by end users. Many radio and television broadcasters provide Internet feeds of their live audio and video productions. They may also allow time-shift viewing or listening such as Preview, Classic Clips and Listen Again features. These providers have been joined by a range of pure Internet "broadcasters" who never had on-air licenses. This means that an Internet-connected device, such as a computer or something more

specific, can be used to access on-line media in much the same way as was previously possible only with a television or radio receiver. The range of available types of content is much wider, from specialized technical webcasts to on-demand popular multimedia services. Podcasting is a variation on this theme, where—usually audio—material is downloaded and played back on a computer or shifted to a portable media player to be listened to on the move. These techniques using simple equipment allow anybody, with little censorship or licensing control, to broadcast audio-visual material worldwide.

Digital media streaming increases the demand for network bandwidth. For example, standard image quality needs 1 Mbps link speed for SD 480p, HD 720p quality requires 2.5 Mbps, and the top-of-the-line HDX quality needs 4.5 Mbps for 1080p.

Webcams are a low-cost extension of this phenomenon. While some webcams can give full-frame-rate video, the picture is usually either small or updates slowly. Internet users can watch animals around an African waterhole, ships in the Panama Canal, traffic at a local roundabout or monitor their own premises, live and in real time. Video chat rooms and video conferencing are also popular with many uses being found for personal webcams, with and without two-way sound. YouTube was founded on 15 February 2005 and is now the leading website for free streaming video with a vast number of users. It uses a flash-based web player to stream and show video files. Registered users may upload an unlimited amount of video and build their own personal profile. YouTube claims that its users watch hundreds of millions, and upload hundreds of thousands of videos daily.

## *Access*




Graph of Internet users per 100 inhabitants between 1997 and 2007 by International Telecommunication Union

The prevalent language for communication on the Internet has been English. This may be a result of the origin of the Internet, as well as the language's role as a lingua franca. Early computer systems were limited to the characters in the American Standard Code for Information Interchange (ASCII), a subset of the Latin alphabet.

After English (27%), the most requested languages on the World Wide Web are Chinese (23%), Spanish (8%), Japanese (5%), Portuguese and German (4% each), Arabic, French and Russian (3% each), and Korean (2%). By region, 42% of the world's Internet users are based in Asia, 24% in Europe, 14% in North America, 10% in Latin America and the Caribbean taken together, 6% in Africa, 3% in the Middle East and 1% in Australia/Oceania. The Internet's technologies have developed enough in recent years, especially in the use of Unicode, that good facilities are available for development and communication in the world's widely used languages. However, some glitches such as *mojibake* (incorrect display of some languages' characters) still remain.

Common methods of Internet access in homes include dial-up, landline broadband (over coaxial cable, fiber optic or copper wires), Wi-Fi, satellite and 3G/4G technology cell phones. Public places to use the Internet include libraries and Internet cafes, where computers with Internet connections are available. There are also Internet access points in

many public places such as airport halls and coffee shops, in some cases just for brief use while standing. Various terms are used, such as "public Internet kiosk", "public access terminal", and "Web payphone". Many hotels now also have public terminals, though these are usually fee-based. These terminals are widely accessed for various usage like ticket booking, bank deposit, online payment etc. Wi-Fi provides wireless access to computer networks, and therefore can do so to the Internet itself. Hotspots providing such access include Wi-Fi cafes, where would-be users need to bring their own wireless-enabled devices such as a laptop or PDA. These services may be free to all, free to customers only, or fee-based. A hotspot need not be limited to a confined location. A whole campus or park, or even an entire city can be enabled. Grassroots efforts have led to wireless community networks. Commercial Wi-Fi services covering large city areas are in place in London, Vienna, Toronto, San Francisco, Philadelphia, Chicago and Pittsburgh. The Internet can then be accessed from such places as a park bench. Apart from Wi-Fi, there have been experiments with proprietary mobile wireless networks like Ricochet, various high-speed data services over cellular phone networks, and fixed wireless services. High-end mobile phones such as smartphones generally come with Internet access through the phone network. Web browsers such as Opera are available on these advanced handsets, which can also run a wide variety of other Internet software. More mobile phones have Internet access than PCs, though this is not as widely used. An Internet access provider and protocol matrix differentiates the methods used to get online.

In contrast, an *Internet blackout* or *outage* can be caused by accidental local signaling interruptions. Disruptions of submarine communications cables may cause blackouts or slowdowns to large areas depending on them, such as in the 2008 submarine cable disruption. Internet blackouts of almost entire countries can be achieved by governments as Internet censorship, such as with the Internet in Egypt, where approximately 93% of networks were shut down in 2011 in an attempt to stop mobilisation for anti-government protests.

In an American study in 2005, the percentage of men using the Internet was very slightly ahead of the percentage of women, although this difference reversed in those under 30. Men logged on more often, spend more time online, and are more likely to be broadband users, whereas women tended to make more use of opportunities to communicate (such as email). Men were more likely to use the Internet to pay bills, participate in auctions, and for recreation such as downloading music and videos. Men and women were equally likely to use the Internet for shopping and banking. More recent studies indicate that in 2008, women significantly outnumbered men on most social networking sites, such as Facebook and Myspace, although the ratios varied with age. In addition, women watched more streaming content, whereas men downloaded more. In terms of blogs, men were more likely to blog in the first place; among those who blog, men were more likely to have a professional blog, whereas women were more likely to have a personal blog.

Overall Internet usage has seen tremendous growth. From 2000 to 2009, the number of Internet users globally rose from 394 million to 1.858 billion.

## *Social impact*

The Internet has enabled entirely new forms of social interaction, activities, and organizing, thanks to its basic features such as widespread usability and access. Social networking websites such as Facebook, Twitter and MySpace have created new ways to socialize and interact. Users of these sites are able to add a wide variety of information to pages, to pursue common interests, and to connect with others. It is also possible to find existing acquaintances, to allow communication among existing groups of people. Sites like LinkedIn foster commercial and business connections. YouTube and Flickr specialize in users' videos and photographs.

In the first decade of the 21st century the first generation is raised with widespread availability of Internet connectivity, bringing consequences and concerns in areas such as personal privacy and identity, and distribution of copyrighted materials. These "digital natives" face a variety of challenges that were not present for prior generations.

The Internet has achieved new relevance as a political tool, leading to Internet censorship by some states. The presidential campaign of Howard Dean in 2004 in the United States was notable for its success in soliciting donation via the Internet. Many political groups use the Internet to achieve a new method of organizing in order to carry out their mission, having given rise to Internet activism. Some governments, such as those of Iran, North Korea, Myanmar, the People's Republic of China, and Saudi Arabia, restrict what people in their countries can access on the Internet, especially political and religious content. This is accomplished through software that filters domains and content so that they may not be easily accessed or obtained without elaborate circumvention.

In Norway, Denmark, Finland and Sweden, major Internet service providers have voluntarily, possibly to avoid such an arrangement being turned into law, agreed to restrict access to sites listed by authorities. While this list of forbidden URLs is only supposed to contain addresses of known child pornography sites, the content of the list is secret. Many countries, including the United States, have enacted laws against the possession or distribution of certain material, such as child pornography, via the Internet, but do not mandate filtering software. There are many free and commercially available software programs, called content-control software, with which a user can choose to block offensive websites on individual computers or networks, in order to limit a child's access to pornographic materials or depiction of violence.

The Internet has been a major outlet for leisure activity since its inception, with entertaining social experiments such as MUDs and MOOs being conducted on university servers, and humor-related Usenet groups receiving much traffic. Today, many Internet forums have sections devoted to games and funny videos; short cartoons in the form of Flash movies are also popular. Over 6 million people use blogs or message boards as a means of communication and for the sharing of ideas. The pornography and gambling industries have taken advantage of the World Wide Web, and often provide a significant source of advertising revenue for other websites. Although many governments have

attempted to restrict both industries' use of the Internet, this has generally failed to stop their widespread popularity.

One main area of leisure activity on the Internet is multiplayer gaming. This form of recreation creates communities, where people of all ages and origins enjoy the fast-paced world of multiplayer games. These range from MMORPG to first-person shooters, from role-playing video games to online gambling. This has revolutionized the way many people interact while spending their free time on the Internet. While online gaming has been around since the 1970s, modern modes of online gaming began with subscription services such as GameSpy and MPlayer. Non-subscribers were limited to certain types of game play or certain games. Many people use the Internet to access and download music, movies and other works for their enjoyment and relaxation. Free and fee-based services exist for all of these activities, using centralized servers and distributed peer-to-peer technologies. Some of these sources exercise more care with respect to the original artists' copyrights than others.

Many people use the World Wide Web to access news, weather and sports reports, to plan and book vacations and to find out more about their interests. People use chat, messaging and email to make and stay in touch with friends worldwide, sometimes in the same way as some previously had pen pals. The Internet has seen a growing number of Web desktops, where users can access their files and settings via the Internet.

Cyberslacking can become a drain on corporate resources; the average UK employee spent 57 minutes a day surfing the Web while at work, according to a 2003 study by Peninsula Business Services. Internet addiction disorder is excessive computer use that interferes with daily life. Some psychologists believe that Internet use has other effects on individuals for instance interfering with the deep thinking that leads to true creativity.

Internet usage has been correlated to users' loneliness.[1] Lonely people tend to use the Internet as an outlet for their feelings and to share their stories with others, such as in the "I am lonely will anyone speak to me" thread.

Chapter 3

# Adaptive Bit Rate

**Adaptive Bitrate Streaming (or Adaptive Streaming)** is a technique used in streaming multimedia over computer networks. While in the past most video streaming technologies utilized streaming protocols such RTSP, today's adaptive streaming technologies are almost exclusively based on HTTP and designed to work efficiently over large distributed HTTP networks such as the Internet.

It works by detecting a user's bandwidth and CPU capacity in real time and adjusting the quality of a video stream accordingly. It requires the use of an encoder which can encode a single source video at multiple bit rates. The player client switches between streaming the different encodings depending on available resources. "The result: very little buffering, fast start time and a good experience for both high-end and low-end connections."

The acronym ABR can be confusing because its most common meaning is "Average bitrate," so it has not been widely adopted by video compression professionals.

## *Current uses*

Post-production houses, content delivery networks and studios use adaptive bit rate technology in order to provide consumers with higher quality video using less manpower and fewer resources. When all is said and done, the creation of multiple video outputs, particularly for adaptive bit rate streaming, adds great value to consumers. If the technology is working as designed, the end user or consumer should be completely unaware of it. Therefore, even though media companies have been actively using adaptive bit rate technology for many years now and it has essentially become a standard practice for high-end streaming providers, mainstream consumers are relatively ignorant of its necessity.

## *Benefits of adaptive bit rate streaming*

Consumers of streaming media experience the highest quality material when adaptive bit rate streaming is used because the user's network and playback conditions are automatically adapted to at any given time under changing conditions.

The media and entertainment industry are the main beneficiaries of adaptive bit rate streaming. As the video space grows exponentially, content delivery networks and video providers can provide customers with a superior viewing experience. Adaptive bit rate technology requires less encoding which simplifies overall workflow and creates better results.

The use of a CDN to deliver media streaming to an Internet audience is often used, as it allows scalability. The CDN received the stream from the source at its Origin server, then replicates it to many or all of its Edge cache servers. The end-user requests the stream and is redirected to the "closest" Edge server. The use of HTTP-base adaptive streaming allows the Edge server to run a simple HTTP server software, whose licence cost is cheap or free, reducing software licencing cost, compared to costly media server licences (eg. Adobe Flash Media Streaming Server). The CDN cost for HTTP streaming media is then similar to HTTP web caching CDN cost.

## *Implementations*

Adaptive bit rate streaming was conceptualized by Move Networks and is now being developed and utilized by Adobe Systems, Apple, Microsoft and Octoshape. In September 2010, Move Networks was awarded a patent for their adaptive bit rate streaming.

### Adobe Dynamic Streaming for Flash

"Dynamic streaming is the process of efficiently delivering streaming video to users by dynamically switching among different streams of varying quality and size during playback. This provides users with the best possible viewing experience their bandwidth and local computer hardware (CPU) can support. Another major goal of dynamic streaming is to make this process smooth and seamless to users, so that if up-scaling or down-scaling the quality of the stream is necessary, it is a smooth and nearly unnoticeable switch without disrupting the continuous playback."

The latest versions of Flash Player and Flash Media Server support adaptive bit-rate streaming over the traditional RTMP protocol, as well as HTTP, similar to the HTTP-based solutions from Apple and Microsoft. HTTP-based streaming has the advantage of not requiring any firewall ports being opened outside of the normal ports used by web browsers. HTTP-based streaming also allows video fragments to be cached by browsers, proxies, and CDNs, drastically reducing the load on the source server.

## Apple HTTP Adaptive Streaming for iPhone/iPad

"HTTP Live Streaming is an HTTP-based media streaming communications protocol implemented by Apple Inc. as part of their QuickTime X, and iPhone software systems." Apple's newly released iPad also provides HTTP Live Streaming capabilities. It works by breaking down streams into several small HTTP-based file downloads that load simultaneously at variable adaptive rates.

HTTP Live Streaming is a standard feature in the iPhone 3.0 and newer versions.

HTTP adaptive bit rate streaming is based on HTTP progressive download, but contrary to the previous approach, here the files are very small, so that they can be compared to the streaming of packets, much like the case of using RTSP and RTP.

While all adaptive bit-rate streaming solutions are proprietary offerings as of October 2010, Apple has submitted its solution to the IETF for consideration as an Internet standard.

## Microsoft Smooth Streaming for Silverlight and Windows Phone 7

Smooth Streaming is an IIS Media Services extension that enables adaptive streaming of media to clients over HTTP.[1] The format specification is based on the ISO Base Media File Format and standardized by Microsoft as the Protected Interoperable File Format. Microsoft is actively involved with 3GPP, MPEG and DECE organizations' efforts to standardize adaptive bit-rate HTTP streaming. Microsoft provides Smooth Streaming Client software development kits for Silverlight and Windows Phone 7. IIS Media Services 4.0, released in November 2010, introduced a feature which enables Smooth Streaming H.264/AAC videos, both live and on-demand, to be dynamically repackaged into the Apple HTTP Adaptive Streaming format and delivered to iOS devices without the need for re-encoding. Microsoft has successfully demonstrated delivery of both live and on-demand 1080p HD video with Smooth Streaming to Silverlight clients. In 2010 Microsoft also partnered with NVIDIA to demonstrate live streaming of 1080p stereoscopic 3D video to PCs equipped with NVIDIA 3D Vision technology.

## Octoshape Multi-BitRate

Octoshape supports automatic mutli-bit rate streaming using standard streaming formats like Flash, Windows and HLS inputs. Octoshape uses a unique throughput optimization technology and resilient coding schemes to maximize the throughput consistency of a video stream over the Internet. Octoshape supports shifting to the appropriate bit rate of the particular consumer of the video. However, the core transport provides for a stable throughput profile over the Internet unlike TCP based technologies like HTTP or RTMP that have variable throughput profiles based on packet loss and latency. The technology selects appropriate bit rates instantly on startup, but rarely makes use of the rate shifting technology during a viewing session, giving the consumer a consistent TV quality video

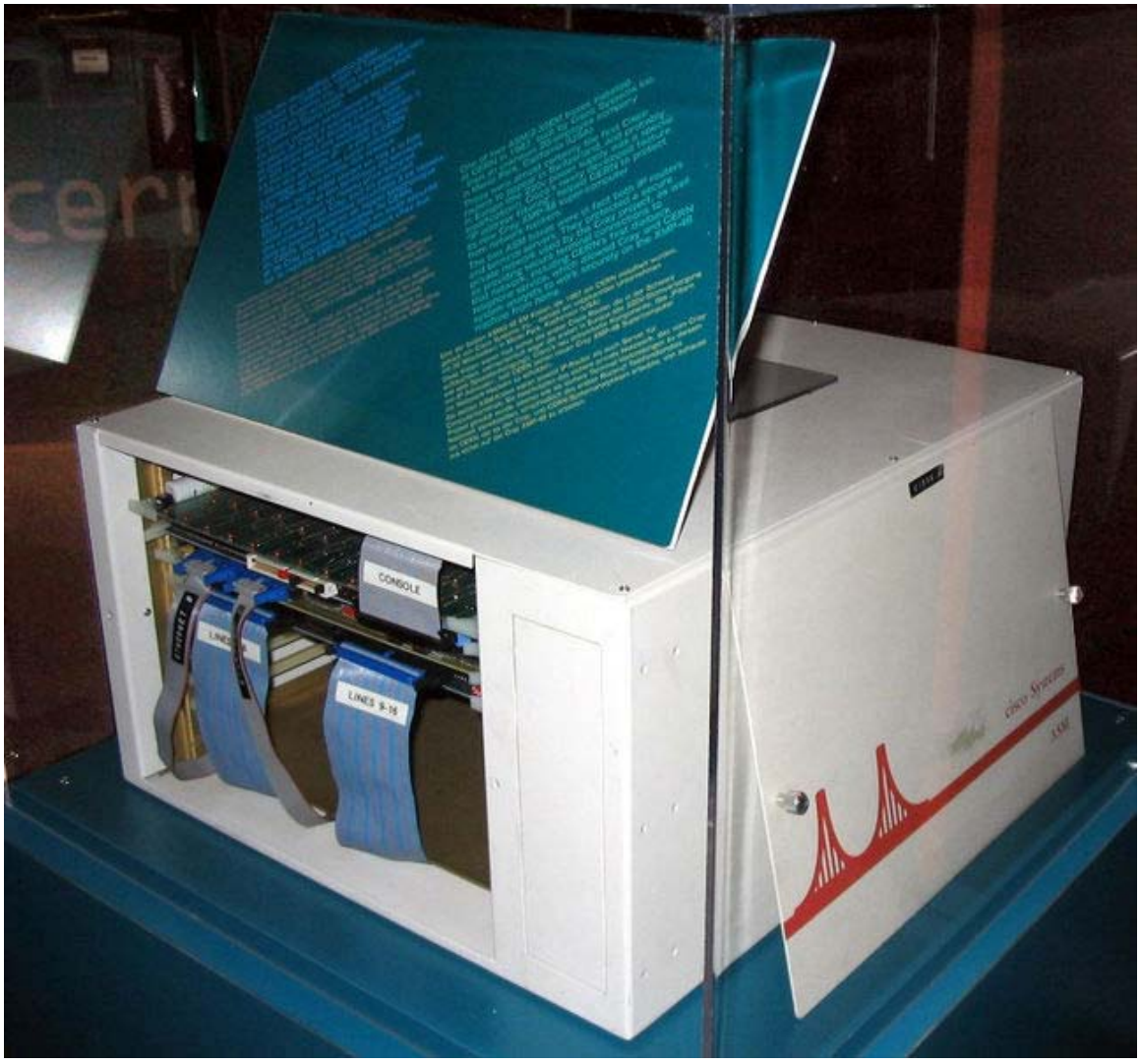
experience. Octoshape is also the first technology to deploy automatic multi-bit rate technology along with Multicast transport over the public Internet.

## *Criticisms*

HTTP based adaptive bit rate technologies are significantly more operationally complex than traditional streaming technologies. Some of the documented considerations are things such as additional storage and encoding costs, and challenges with maintaining quality globally. There have also been some interesting dynamics found around the interactions between complex adaptive bit rate logic competing with complex TCP flow control logic.

**Chapter 4**

# Router




A Cisco ASM/2-32EM router deployed at CERN in 1987


Juniper SRX210 service gateway router

A **router** is a device that forwards data packets across computer networks. Routers perform the data "traffic directing" functions on the Internet. A router is a microprocessor-controlled device that is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table, it directs the packet to the next network on its journey. A data packet is typically passed from router to router through the networks of the Internet until it gets to its destination computer. Routers also perform other tasks such as translating the data transmission protocol of the packet to the appropriate protocol of the next network, and preventing unauthorized access to a network by the use of a firewall.

The most familiar type of routers are home and small office routers that simply pass data, such as web pages and email, between the home computers and the owner's cable or DSL modem, which connects to the Internet (ISP). However more sophisticated routers range from enterprise routers, which 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.

## *Applications*

When multiple routers are used in interconnected networks, the routers exchange information about destination addresses, using a dynamic routing protocol. Each router builds up a table listing the preferred routes between any two systems on the interconnected networks. A router has interfaces for different physical types of network connections, (such as copper cables, fiber optic, or wireless transmission). It also contains firmware for different networking protocol standards. Each network interface uses 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 sub-network address. The subnets addresses recorded in the router do not necessarily map directly to the physical interface connections. A router has two stages of operation called planes:

- Control plane: A router records a routing table listing what route should be used to forward a data packet, and through which physical interface connection. It does this using internal pre-configured addresses, called static routes.


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

- Forwarding plane: The router forwards data packets between incoming and outgoing interface connections. It routes it to the correct network type using information that the packet header contains. It uses data recorded in the routing table control plane.

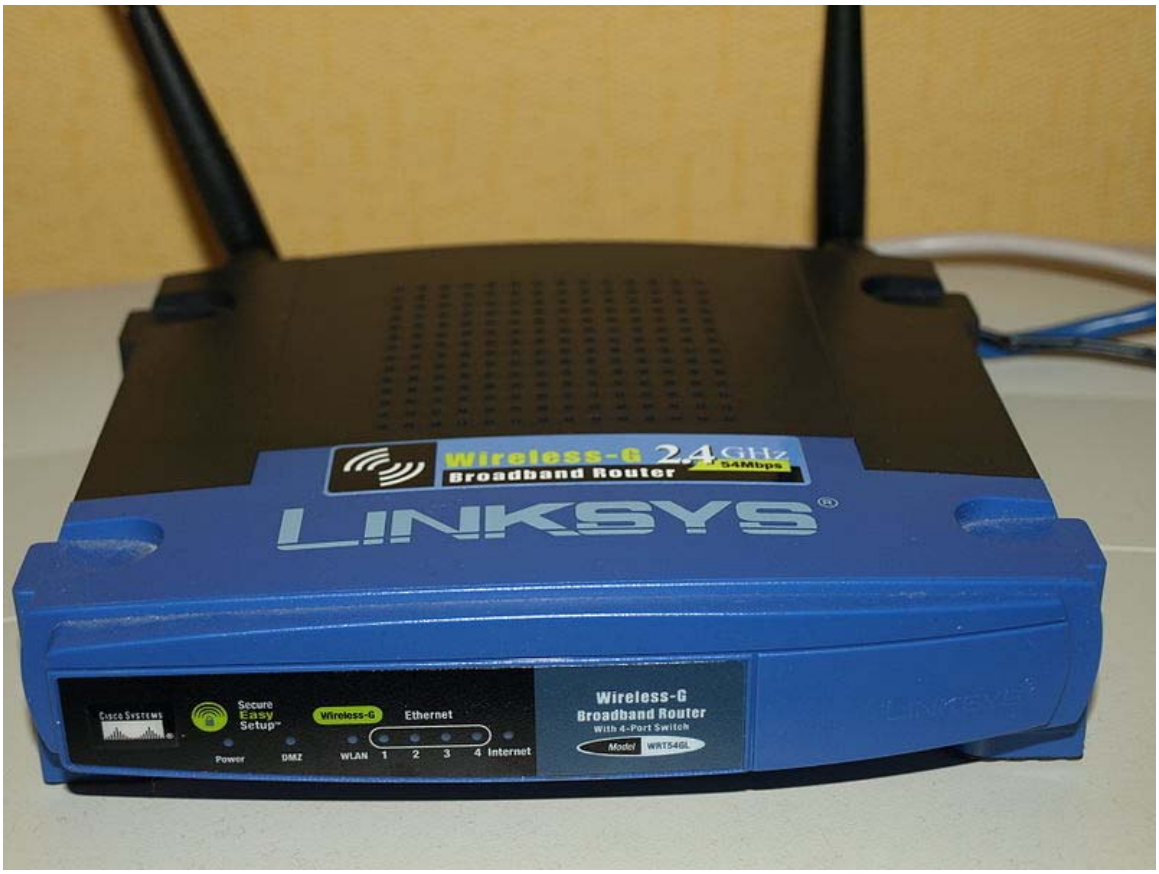
Routers may provide connectivity within enterprises, between enterprises and the Internet, and between internet service providers (ISPs) networks. The largest routers (such as the Cisco CRS-1 or Juniper T1600) interconnect the various ISPs, or may be used in large enterprise networks. Smaller routers 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.

## Enterprise routers

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




Linksys by Cisco WRT54GL SoHo Router


A screenshot of the LuCI web interface used by OpenWrt. Here it is being used to configure 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 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. Separate from the router may be a firewall or VPN handling device, or the router may include these and other security functions. Many companies produced security-oriented routers, including Cisco Systems' PIX and ASA5500 series, Juniper's Netscreen, Watchguard's Firebox, Barracuda's variety of mail-oriented devices, and many others.

## 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.

## Internet connectivity and internal use

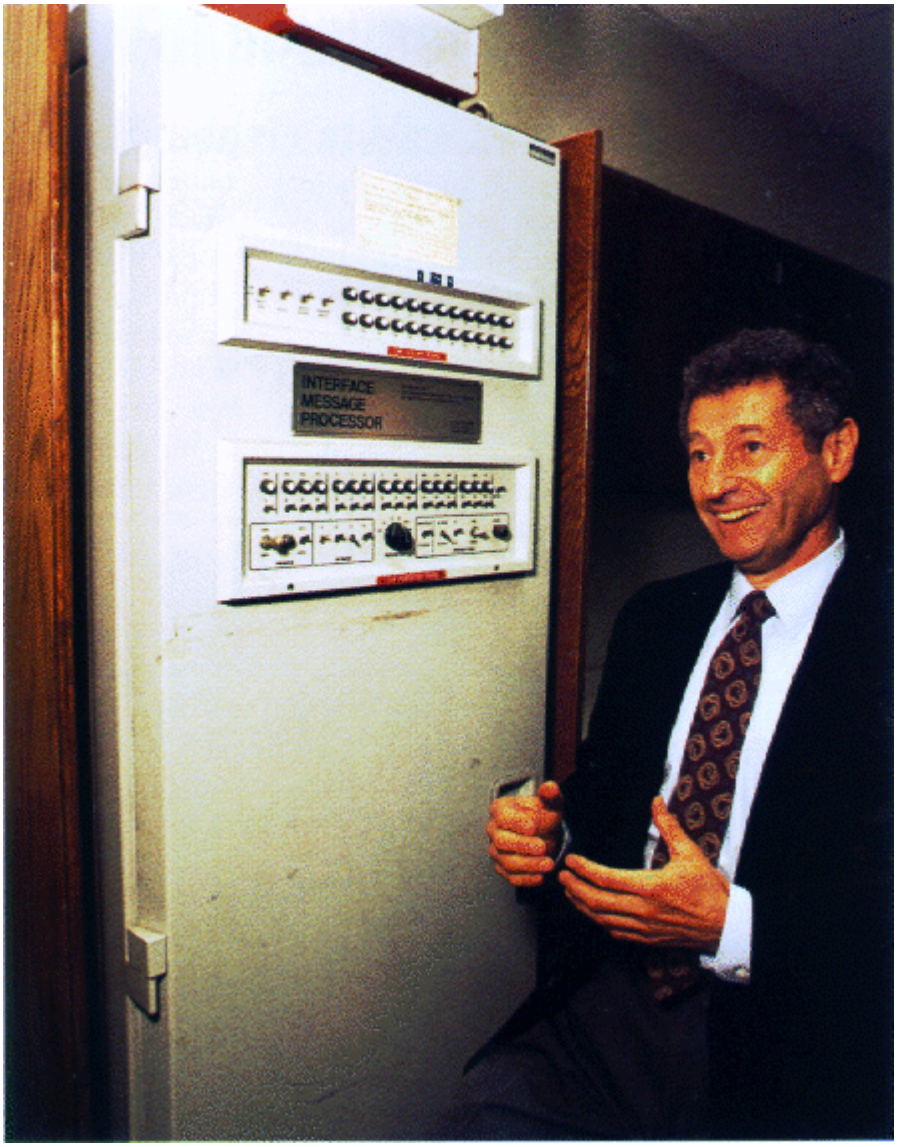
Routers intended for ISP and major enterprise connectivity usually exchange routing information using the Border Gateway Protocol (BGP). RFC 4098 standard defines the types of BGP-protocol routers according to the routers' functions:

- *Edge router*: Also called a Provider Edge router, is placed at the edge of an ISP network. The router uses External BGP to EBGP protocol 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 protocol to its provider's Autonomous System. It is typically used in an (enterprise) organization.
- *Inter-provider border router*: Interconnecting ISPs, is a BGP-protocol router that maintains BGP sessions with other BGP protocol 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.]

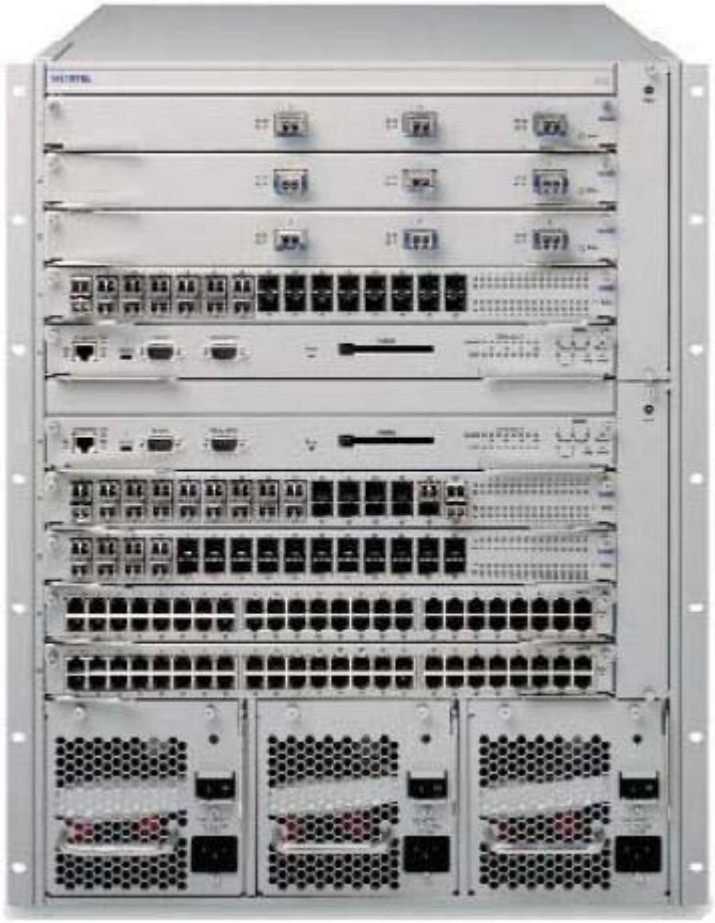
  Within an ISP: In the ISPs Autonomous System, a router uses internal BGP protocol to communicate with other ISP edge routers, other intranet core routers, or the ISPs intranet provider border routers.
  "Internet backbone:" The Internet no longer has a clearly identifiable backbone, unlike its predecessor networks. 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-protocol 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,. Voice traffic that the traditional cable networks once carried. 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.




Leonard Kleinrock and the first IMP.



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 packet 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 networks 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 (this particular idea had been previously pioneered in the CYCLADES network).

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.

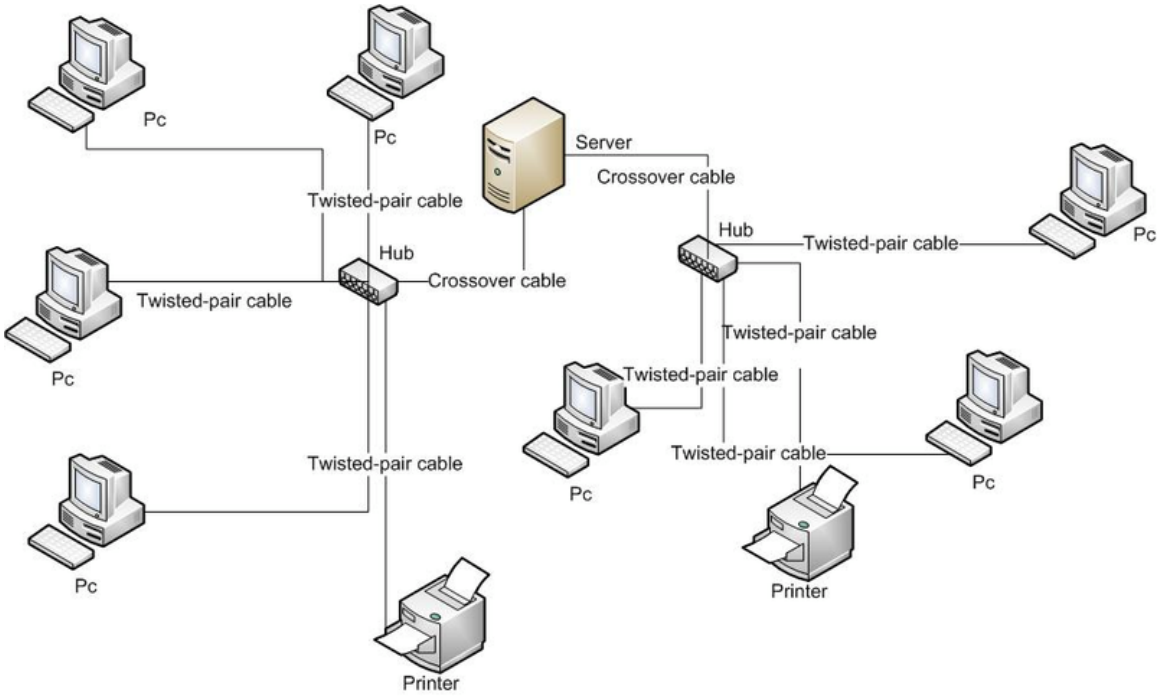
The first multiprotocol routers were independently created by staff researchers at MIT and Stanford in 1981; the Stanford router was done by William Yeager, and the MIT one by Noel Chiappa; both were also based on PDP-11s.

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*




Computer network

For pure Internet Protocol (IP) forwarding function, a router is designed to minimize the state information associated with individual packets. 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. This process is known as routing. When each 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 network addresses in the routing table. Once a match is found, the packet is encapsulated in the Layer 2 data link frame for that outgoing interface. A router does not look into the actual data contents that the packet carries, but only at the layer 3 addresses to make a forwarding decision, plus optionally other information in the header for hint on, for example, QoS. Once a packet is forwarded, the router does not retain any historical information about the packet, but the forwarding action can be collected into the statistical data, if so configured.

Forwarding decisions can involve decisions at layers other than layer 3. A function that forwards based on layer 2 information, is properly called a bridge. This function is referred to as layer 2 bridging, as the addresses it uses to forward the traffic are layer 2 addresses (e.g. MAC addresses on Ethernet).

Besides making decision as 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 packets once the length of the queue exceeds the size of the buffers in the router. RED probabilistically drops datagrams early when the queue is exceeds a pre-configured size of the queue until a pre-configured 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 quality of service (QoS), which is critical when Voice over IP is deployed, so that delays between packets do not exceed 150ms to maintain the quality of voice conversations.

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.

These 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 caused by multiple CPU cycles, and others may have to be performed through the CPU as these packets need special attention that cannot be handled by an ASIC.

Chapter 5

# Bridging (Networking)

**Bridging** is a forwarding technique used in packet-switched computer networks. Unlike routing, bridging makes no assumptions about where in a network a particular address is located. Instead, it depends on flooding and examination of source addresses in received packet headers to locate unknown devices. Once a device has been located, its location is recorded in a table where the MAC address is stored so as to preclude the need for further broadcasting. The utility of bridging is limited by its dependence on flooding, and is thus only used in local area networks.

Bridging generally refers to *Transparent bridging* or *Learning bridge* operation which predominates in Ethernet. Another form of bridging, Source route bridging, was developed for token ring networks.

A **network bridge** connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term *bridge* formally means a device that behaves according to the IEEE 802.1D standard. A bridge and switch are very much alike; a switch being a bridge with numerous ports. *Switch* or *Layer 2 switch* is often used interchangeably with *bridge*.

Bridges are similar to repeaters or network hubs, devices that connect network segments at the physical layer (Layer 1) of the OSI model; however, with bridging, traffic from one network is managed rather than simply rebroadcasted to adjacent network segments. Bridges are more complex than hubs or repeaters. Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.

## *Transparent bridging operation*

A bridge uses a forwarding database to send frames across network segments. The forwarding database is initially empty and entries in the database are built as the bridge

receives frames. If an address entry is not found in the forwarding database, the frame is flooded to all other ports of the bridge, forwarding the frame to all segments except the source address. By means of these broadcast frames, the destination network will respond and forwarding database entry will be created.

As an example, consider three hosts, A, B and C and a bridge. The bridge has three ports. A is connected to bridge port 1, B is connected bridge port 2, C is connected to bridge port 3. A sends a frame addressed to B to the bridge. The bridge examines the source address of the frame and creates an address and port number entry for A in its forwarding table. The bridge examines the destination address of the frame and does not find it in its forwarding table so it floods it to all other ports: 2 and 3. The frame is received by hosts B and C. Host C examines the destination address and ignores the frame. Host B recognizes a destination address match and generates a response to A. On the return path, the bridge adds an address and port number entry for B to its forwarding table. The bridge already has A's address in its forwarding table so it forwards the response only to port 1. Host C or any other hosts on port 3 are not burdened with the response. Two-way communication is now possible between A and B without any further flooding.

Note that both source and destination addresses are used in this algorithm. Source addresses are recorded in entries in the table, while destination addresses are looked up in the table and matched to the proper segment to send the frame to.

The technology was originally developed by the Digital Equipment Corp. in the 1980s.

## Filtering database

To translate between two segments, a bridge reads a frame's destination MAC address and decides to either forward or filter. If the bridge determines that the destination node is on another segment on the network, it forwards (retransmits) the packet to that segment. If the destination address belongs to the same segment as the source address, the bridge filters (discards) the frame. As nodes transmit data through the bridge, the bridge establishes a filtering database (also known as a forwarding table) of known MAC addresses and their locations on the network. The bridge uses its filtering database to determine whether a packet should be forwarded or filtered.

## Destination lookup failure

Layer 2 (L2) Ethernet Switch is looking at the MAC Destination address of the Ethernet frame in order to switch it to the appropriate port/s. In case that MAC address exists in the Switch L2 Table, it transmits the Frame only to the port which is tied to that entry. In case that MAC address doesn’t exist in the Switch L2 Table, the frame is considered DLF and it been transmitted to all forwarding ports of that VLAN. (Also Broadcasts such as ARP Request messages are transmitted to the same ports)

## *Advantages of network bridges*

- Self-configuring
- Simple bridges are inexpensive
- Isolate collision domain
- Reduce the size of collision domain by microsegmentation in non-switched networks
- Transparent to protocols above the MAC layer
- Allows the introduction of management/performance information and access control
- LANs interconnected are separate, and physical constraints such as number of stations, repeaters and segment length don't apply
- Helps minimize bandwidth usage

## *Disadvantages of network bridges*

- Does not limit the scope of broadcasts [broadcast domain cannot be controlled]
- Does not scale to extremely large networks
- Buffering and processing introduces delays
- Bridges are more expensive than repeaters or hubs
- A complex network topology can pose a problem for transparent bridges. For example, multiple paths between transparent bridges and LANs can result in *bridge loops*. The spanning tree protocol helps to reduce problems with complex topologies.

## *Bridging versus routing*

Bridging and routing are both ways of performing data control, but work through different methods. Bridging takes place at OSI Model Layer 2 (data-link layer) while routing takes place at the OSI Model Layer 3 (network layer). This difference means that a bridge directs frames according to hardware assigned MAC addresses while a router makes its decisions according to arbitrarily assigned IP Addresses. As a result of this, bridges are not concerned with and are unable to distinguish networks while routers can.

When designing a network, one can choose to put multiple segments into one bridged network or to divide it into different networks interconnected by routers. If a host is physically moved from one network area to another in a routed network, it has to get a new IP address; if this system is moved within a bridged network, it doesn't have to reconfigure anything.

**Chapter 6**

# Network Switch


Typical SOHO network switch.


Back view of Atlantis network switch with Ethernet ports.

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

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

The term **network switch** does not generally encompass unintelligent or passive network devices such as hubs and repeaters.

The first Ethernet switch was introduced by Kalpana in 1990.

## *Function*

The network switch plays an integral part in most modern Ethernet local area networks (LANs). Mid-to-large sized LANs contain a number of linked managed switches. Small office/home office (SOHO) applications typically use a single switch, or an all-purpose converged device such as a gateway to access small office/home broadband services such as DSL or cable internet. In most of these cases, the end-user device contains a router and

components that interface to the particular physical broadband technology. User devices may also include a telephone interface for VoIP.

An Ethernet switch operates at the data link layer of the OSI model to create a separate collision domain for each switch port. With 4 computers (e.g., A, B, C, and D) on 4 switch ports, A and B can transfer data back and forth, while C and D also do so simultaneously, and the two conversations will not interfere with one another. In the case of a hub, they would all share the bandwidth and run in half duplex, resulting in collisions, which would then necessitate retransmissions. Using a switch is called microsegmentation. This allows computers to have dedicated bandwidth on a point-to-point connections to the network and to therefore run in Full duplex without collisions.

## *Role of switches in networks*

Switches may operate at one or more layers of the OSI model, including data link, network, or transport (i.e., end-to-end). A device that operates simultaneously at more than one of these layers is known as a multilayer switch.

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

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

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

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

## *Layer-specific functionality*


A modular network switch with three network modules (a total of 24 Ethernet and 14 Fast Ethernet ports) and one power supply.

While switches may learn about topologies at many layers, and forward at one or more layers, they do tend to have common features. Other than for high-performance applications, modern commercial switches use primarily Ethernet interfaces, which can have different input and output bandwidths of 10, 100, 1000 or 10,000 megabits per second.

At any layer, a modern switch may implement power over Ethernet (PoE), which avoids the need for attached devices, such as an VoIP phone or wireless access point, to have a separate power supply. Since switches can have redundant power circuits connected to uninterruptible power supplies, the connected device can continue operating even when regular office power fails.

## Layer 1 hubs versus higher-layer switches

A network hub, or repeater, is a simple network device. Hubs do not manage any of the traffic that comes through them. Any packet entering a port is broadcast out or "repeated" on every other port, except for the port of entry. Since every packet is repeated on every other port, packet collisions result, which slows down the network.

There are specialized applications where a hub can be useful, such as copying traffic to multiple network sensors. High end switches have a feature which does the same thing called port mirroring.

There is no longer any significant price difference between a hub and a low-end switch.

## Layer 2

A network bridge, operating at the data link layer, may interconnect a small number of devices in a home or the office. This is a trivial case of bridging, in which the bridge learns the MAC address of each connected device.

Single bridges also can provide extremely high performance in specialized applications such as storage area networks.

Classic bridges may also interconnect using a spanning tree protocol that disables links so that the resulting local area network is a tree without loops. In contrast to routers, spanning tree bridges must have topologies with only one active path between two points. The older IEEE 802.1D spanning tree protocol could be quite slow, with forwarding stopping for 30 seconds while the spanning tree would reconverge. A Rapid Spanning Tree Protocol was introduced as IEEE 802.1w, but the newest edition of IEEE 802.1D adopts the 802.1w extensions as the base standard.

The IETF is specifying the TRILL protocol, which is the application of link-state routing technology to the layer-2 bridging problem. Devices which implement TRILL, called RBridges, combine the best features of both routers and bridges.

While "layer 2 switch" remains more of a marketing term than a technical term, the products that were introduced as "switches" tended to use microsegmentation and Full duplex to prevent collisions among devices connected to Ethernet. By using an internal forwarding plane much faster than any interface, they give the impression of simultaneous paths among multiple devices.

Once a bridge learns the topology through a spanning tree protocol, it forwards data link layer frames using a layer 2 forwarding method. There are four forwarding methods a bridge can use, of which the second through fourth method were performance-increasing methods when used on "switch" products with the same input and output port bandwidths:

1. Store and forward: The switch buffers and verifies each frame before forwarding it.
2. Cut through: The switch reads only up to the frame's hardware address before starting to forward it. Cut-through switches have to fall back to store and forward if the outgoing port is busy at the time the packet arrives. There is no error checking with this method.
3. Fragment free: A method that attempts to retain the benefits of both store and forward and cut through. Fragment free checks the first 64 bytes of the frame, where addressing information is stored. According to Ethernet specifications, collisions should be detected during the first 64 bytes of the frame, so frames that are in error because of a collision will not be forwarded. This way the frame will always reach its intended destination. Error checking of the actual data in the packet is left for the end device.
4. Adaptive switching: A method of automatically selecting between the other three modes.

While there are specialized applications, such as storage area networks, where the input and output interfaces are the same bandwidth, this is rarely the case in general LAN applications. In LANs, a switch used for end user access typically concentrates lower bandwidth (e.g., 10/100 Mbit/s) into a higher bandwidth (at least 1 Gbit/s). Alternatively, a switch that provides access to server ports usually connects to them at a much higher bandwidth than is used by end user devices.

## Layer 3

Within the confines of the Ethernet physical layer, a layer 3 switch can perform some or all of the functions normally performed by a router. The most common layer-3 capability is awareness of IP multicast through IGMP snooping. With this awareness, a layer-3 switch can increase efficiency by delivering the traffic of a multicast group only to ports where the attached device has signaled that it wants to listen to that group.

## Layer 4

While the exact meaning of the term Layer-4 switch is vendor-dependent, it almost always starts with a capability for network address translation, but then adds some type of load distribution based on TCP sessions.

The device may include a stateful firewall, a VPN concentrator, or be an IPSec security gateway.

## Layer 7

Layer 7 switches may distribute loads based on URL or by some installation-specific technique to recognize application-level transactions. A Layer-7 switch may include a web cache and participate in a content delivery network.

Rack-mounted 24-port 3Com switch

## *Types of switches*

### Form factor

- Desktop, not mounted in an enclosure, typically intended to be used in a home or office environment outside of a wiring closet
- Rack mounted
- Chassis — with swappable "switch module" cards. e.g. Alcatel's OmniSwitch 9000; Cisco Catalyst switch 4500 and 6500; 3Com 7700, 7900E, 8800.
- DIN rail mounted, normally seen in industrial environments or panels

### Configuration options

- *Unmanaged* switches — These switches have no configuration interface or options. They are plug and play. They are typically the least expensive switches, found in home, SOHO, or small businesses. They can be desktop or rack mounted.
- *Managed* switches — These switches have one or more methods to modify the operation of the switch. Common management methods include: a command-line interface (CLI) accessed via serial console, telnet or Secure Shell, an embedded

Simple Network Management Protocol (SNMP) agent allowing management from a remote console or management station, or a web interface for management from a web browser. Examples of configuration changes that one can do from a managed switch include: enable features such as Spanning Tree Protocol, set port bandwidth, create or modify Virtual LANs (VLANs), etc. Two sub-classes of managed switches are marketed today:

- *Smart* (or intelligent) switches — These are managed switches with a limited set of management features. Likewise "web-managed" switches are switches which fall in a market niche between unmanaged and managed. For a price much lower than a fully managed switch they provide a web interface (and usually no CLI access) and allow configuration of basic settings, such as VLANs, port-bandwidth and duplex.
- *Enterprise Managed* (or fully managed) switches — These have a full set of management features, including CLI, SNMP agent, and web interface. They may have additional features to manipulate configurations, such as the ability to display, modify, backup and restore configurations. Compared with smart switches, enterprise switches have more features that can be customized or optimized, and are generally more expensive than smart switches. Enterprise switches are typically found in networks with larger number of switches and connections, where centralized management is a significant savings in administrative time and effort. A stackable switch is a version of enterprise-managed switch.

## Traffic monitoring on a switched network

Unless port mirroring or other methods such as RMON or SMON are implemented in a switch,[1] it is difficult to monitor traffic that is bridged using a switch because only the sending and receiving ports can see the traffic. These monitoring features are rarely present on consumer-grade switches.

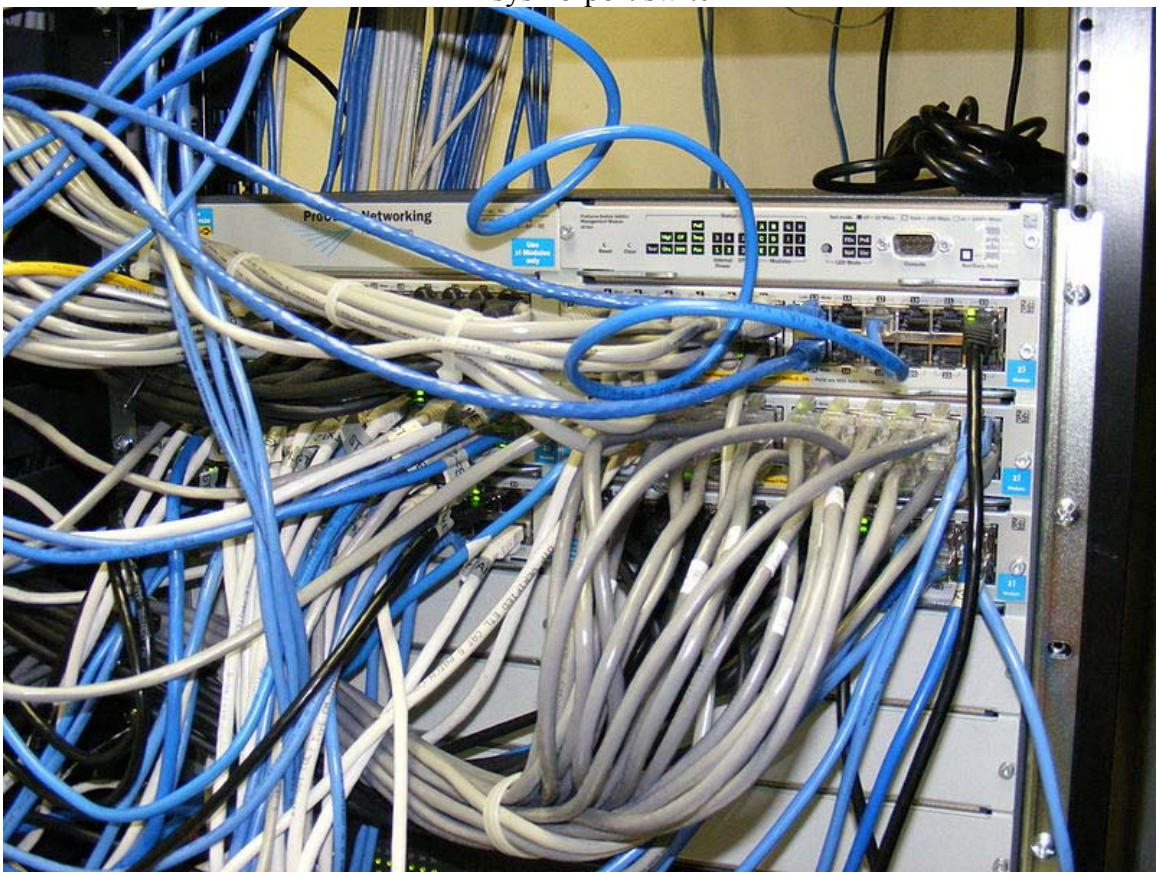
Two popular methods that are specifically designed to allow a network analyst to monitor traffic are:

- Port mirroring — the switch sends a copy of network packets to a monitoring network connection.
- SMON — "Switch Monitoring" is described by RFC 2613 and is a protocol for controlling facilities such as port mirroring.

Another method to monitor may be to connect a Layer-1 hub between the monitored device and its switch port. This will induce minor delay, but will provide multiple interfaces that can be used to monitor the individual switch port.

## Typical switch management features

Linksys 48-port switch



HP Procurve rack-mounted switches Mounted in a standard 19inch Telco Rack 19-inch rack with network cables

- Turn particular port range on or off
- Link bandwidth and duplex settings
- Priority settings for ports
- MAC filtering and other types of "port security" features which prevent MAC flooding
- Use of Spanning Tree Protocol
- SNMP monitoring of device and link health
- Port mirroring (also known as: port monitoring, spanning port, SPAN port, roving analysis port or link mode port)
- Link aggregation (also known as *bonding*, *trunking* or *teaming*)
- VLAN settings
- 802.1X network access control
- IGMP snooping

Link aggregation allows the use of multiple ports for the same connection achieving higher data transfer rates. Creating VLANs can serve security and performance goals by reducing the size of the broadcast domain.

**Chapter 7**

# Network Interface Controller & Ethernet Hub

## Network Interface Controller

Network Interface Card (NIC)

A 1990s Ethernet network interface controller card which connects to the motherboard via the now-obsolete ISA bus. This combination card features both a (now obsolete) bayonet cap BNC connector (left) for use in coaxial-based 10base2 networks and an RJ-45 connector (right) for use in twisted pair-based 10baseT networks. (The ports could not be used simultaneously.)

**Connects to**

Motherboard via one of:

- Integrated
- PCI Connector
- ISA Connector
- PCI-E
- FireWire
- USB

Network via one of:

- Fast Ethernet

- Gigabit Ethernet
- Optical fiber
- Token ring

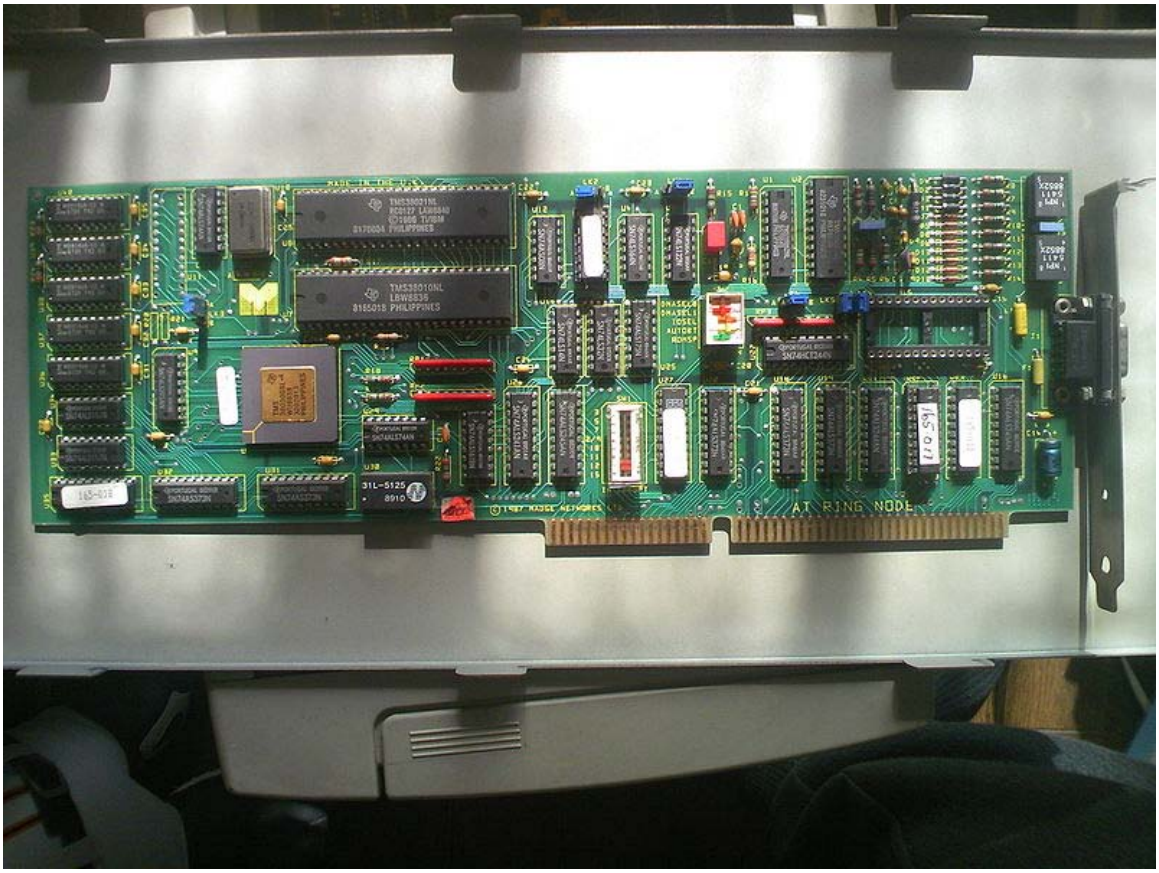
| | |
|---|---|
| **Speeds** | 10 Mbit/s<br>100 Mbit/s<br>1000 Mbit/s<br>up to 160 Gbit/s |
| **Common manufacturers** | Novell<br>Intel<br>Realtek<br>Others |

A **network interface controller** (also known as a **network interface card**, **network adapter**, **LAN adapter** and by similar terms) is a computer hardware component that connects a computer to a computer network.

Whereas network interface controllers were commonly implemented on expansion cards that plug into a computer bus, the low cost and ubiquity of the Ethernet standard means that most newer computers have a network interface built into the motherboard.

## *Purpose*

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




Madge 4/16Mbps TokenRing ISA NIC

Although other network technologies exist (e.g. token ring), Ethernet has achieved near-ubiquity since the mid-1990s.

Every Ethernet network controller has a unique 48-bit serial number called a MAC address, which is stored in read-only memory carried on the card for add-on cards. Every computer on an Ethernet network must have at least one controller. Each controller must have a unique MAC address. Normally it is safe to assume that no two network controllers will share the same address, because controller vendors purchase blocks of addresses from the Institute of Electrical and Electronics Engineers (IEEE) and assign a unique address to each controller at the time of manufacture.

The NIC allows computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

## *Implementation*

Whereas network controllers used to be expansion cards that plugged into a computer bus, the low cost and ubiquity of the Ethernet standard means that most newer computers have a network interface built into the motherboard. Newer server motherboards may even have dual network interfaces built-in. The Ethernet capabilities are either integrated into the motherboard chipset or implemented via a low cost dedicated Ethernet chip, connected through the PCI (or the newer PCI express) bus. A separate network card is not required unless additional interfaces are needed or some other type of network is used.

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

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

An Ethernet network controller typically has a RJ45 socket where the network cable is connected. Older NICs also supplied BNC, or AUI connections. A few LEDs inform the user of whether the network is active, and whether or not there is data being transmitted on it. Ethernet network controllers typically support 10 Mbit/s Ethernet, 100 Mbit/s Ethernet, and 1000 Mbit/s Ethernet varieties. Such controllers are designated *10/100/1000* and this means they can support a notional maximum transfer rate of 10, 100 or 1000 Megabits per second.

# Ethernet Hub


4-port Ethernet hub

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

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

## *Technical information*

A network hub is a fairly unsophisticated broadcast device. Hubs do not manage any of the traffic that comes through them, and any packet entering any port is regenerated and broadcast out on all other ports. Since every packet is being sent out through all other ports, packet collisions result—which greatly impedes the smooth flow of traffic.

100 Mbit/s hubs/repeater come in two different speed grades: Class I delay the signal for a maximum of 140 bit times (enabling translation between 100Base-TX, 100Base-FX and 100Base-T4) and Class II ones delay the signal for a maximum of 92 bit times (enabling installation of two hubs in a single collision domain).

The need for hosts to be able to detect collisions limits the number of hubs and the total size of a network built using hubs (a network built using switches does not have these limitations). For 10 Mbit/s networks built using repeater hubs, the 5-4-3 rule must be followed: up to 5 segments (4 hubs) are allowed between any two end stations. For 100 Mbit/s networks, the limit is reduced to 3 segments (2 hubs) between any two end stations, and even that is only allowed if the hubs are of Class II. Some hubs have manufacturer specific stack ports allowing them to be combined in a way that allows more hubs than simple chaining through Ethernet cables, but even so, a large fast Ethernet network is likely to require switches to avoid the chaining limits of hubs.

Most hubs detect typical problems, such as excessive collisions and jabbering on individual ports, and *partition* the port, disconnecting it from the shared medium. Thus, hub-based Ethernet is generally more robust than coaxial cable-based Ethernet (e.g. 10BASE2), where a misbehaving device can adversely affect the entire collision domain. Even if not partitioned automatically, a hub simplifies troubleshooting because they remove the need to troubleshoot faults on a long cable with multiple taps; status lights on the hub can indicate the possible problem source or, as a last resort, devices can be disconnected from a hub one at a time much more easily than from a coaxial cable.

Hubs are classified as Layer 1 (physical layer) devices in the OSI model. At the physical layer, hubs support little in the way of sophisticated networking. Hubs do not read any of the data passing through them and are not aware of their source or destination. A hub simply receives incoming Ethernet frames, regenerates the electrical signal, and broadcasts these packets out to all other devices on the network.

To pass data through the repeater in a usable fashion from one segment to the next, the packets and the Logical Link Control (LLC) protocols must be the same on the each segment. This means that a repeater will not enable communication, for example, between an 802.3 segment (Ethernet) and an 802.5 segment (Token Ring). That is, they cannot translate an Ethernet packet into a Token Ring packet. In other words, repeaters do not translate anything.

## *Dual speed hubs*

In the early days of fast Ethernet, Ethernet switches were relatively expensive devices. Hubs suffered from the problem that if there were any 10BASE-T devices connected then the whole network needed to run at 10 Mbit/s. Therefore a compromise between a hub and a switch was developed, known as a **dual-speed hub**. These devices consisted of an internal two-port switch, dividing the 10 Mbit/s and 100 Mbit/s segments. The device would typically consist of more than two physical ports. When a network device becomes active on any of the physical ports, the device attaches it to either the 10 Mbit/s segment or the 100 Mbit/s segment, as appropriate. This prevented the need for an all-or-nothing migration fast Ethernet networks. These devices are considered hubs because the traffic between devices connected at the same speed is not switched.

## *Uses*

Historically, the main reason for purchasing hubs rather than switches was their price. This motivator has largely been eliminated by reductions in the price of switches, but hubs can still be useful in special circumstances:

- For inserting a protocol analyzer into a network connection, a hub is an alternative to a network tap or port mirroring.
- When a switch is accessible for end users to make connections, for example, in a conference room, an inexperienced or careless user (or saboteur) can bring down the network by connecting two ports together, causing a loop. This can be prevented by using a hub, where a loop will break other users on the hub, but not the rest of the network. This hazard can also be avoided by using switches that can detect and deal with loops, for example by implementing the spanning tree protocol.
- A hub with a 10BASE2 port can be used to connect devices that only support 10BASE2 to a modern network. The same goes for linking in an old 10BASE5 network segment using an AUI port on a hub (individual devices that were intended for thicknet can be linked to modern Ethernet by using an AUI-10BASE-T transceiver).

Chapter 8

# Modem

A **modem** (**mo**dulator-**dem**odulator) is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal 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 over any means of transmitting analog signals, from driven diodes to radio.

The most familiar example is a voice band modem that turns the digital data of a personal computer into modulated electrical signals in the voice frequency range of a telephone channel. These signals can be transmitted 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 time unit, normally measured in bits per second (bit/s, or bps). They can also be classified by the symbol rate measured in baud, the number of times the modem changes its signal state per second. For example, the ITU V.21 standard used audio frequency-shift keying, aka tones, to carry 300 bit/s using 300 baud, whereas the original ITU V.22 standard allowed 1,200 bit/s with 600 baud using phase shift keying.

## *History*

News wire services in 1920s used multiplex equipment that met the definition, but the modem function was incidental to the multiplexing function, so they are not commonly included in the history of modems.

TeleGuide terminal

Modems grew out of the need to connect teletype machines over ordinary phone lines instead of more expensive leased lines which had previously been used for current loop-based teleprinters and automated telegraphs. George Stibitz connected a New Hampshire teletype to a computer in New York City by a subscriber telephone line in 1940.

In 1943, IBM adapted this technology to their unit record equipment and were able to transmit punched cards at 25 bits/second. Mass-produced modems in the United States began as part of the SAGE air-defense system in 1958, 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.

In the summer of 1960, the name *Data-Phone* was introduced to replace the earlier term *digital subset*. The *202 Data-Phone* was a half-duplex asynchronous service that was marketed extensively in late 1960. In 1962, the *201A* and *201B Data-Phones* were introduced. They 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 running on their own set of two wires each.

The famous *Bell 103A dataset* standard was also introduced by Bell Labs in 1962. It provided full-duplex service at 300 baud 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 KSR33, the ASR33, and the IBM 2741. AT&T reduced modem costs by introducing the originate-only 113D and the answer-only 113B/C modems.

## The Carterfone decision


The *Novation CAT* acoustically coupled modem

For many years, the Bell System (AT&T) maintained a monopoly on the use of its phone lines, allowing only Bell-supplied devices to be attached to its network. Before 1968, AT&T maintained a monopoly on what devices could be *electrically* connected to its phone lines. This led to a market for 103A-compatible modems that were *mechanically* connected to the phone, through the handset, known as acoustically coupled modems. Particularly common models from the 1970s were the Novation CAT and the Anderson-Jacobson, spun off from an in-house project at Stanford Research Institute (now SRI

International). Hush-a-Phone v. FCC was a seminal ruling in United States telecommunications law decided by the DC Circuit Court of Appeals on November 8, 1956. The District Court found that it was within the FCC's authority to regulate the terms of use of AT&T's equipment. Subsequently, the FCC examiner found that as long as the device was not physically attached it would not threaten to degenerate the system. Later, in the Carterfone decision of 1968, the FCC passed a rule setting stringent AT&T-designed tests for electronically coupling a device to the phone lines. AT&T's tests were complex, making electronically-coupled modems expensive, so acoustically-coupled modems remained common into the early 1980s.

In December 1972, Vadic introduced the *VA3400*. This device was remarkable because it provided full duplex operation at 1,200 bit/s over the dial network, using methods similar to those of the 103A in that 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 to Vadic's model, but used the lower frequency set for transmission. It was also possible to 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.

## The Smartmodem and the rise of BBSes

US Robotics Sportster 14,400 Fax modem (1994)

The next major advance in modems was the *Smartmodem*, introduced in 1981 by Hayes Communications. The Smartmodem was an otherwise standard 103A 300-bit/s modem, but was attached to a small controller that let the computer send commands to it and enable it to operate the phone line. The command set included instructions for picking up and hanging up the phone, dialing numbers, and answering calls. The basic Hayes command set remains the basis for computer control of most modern modems.

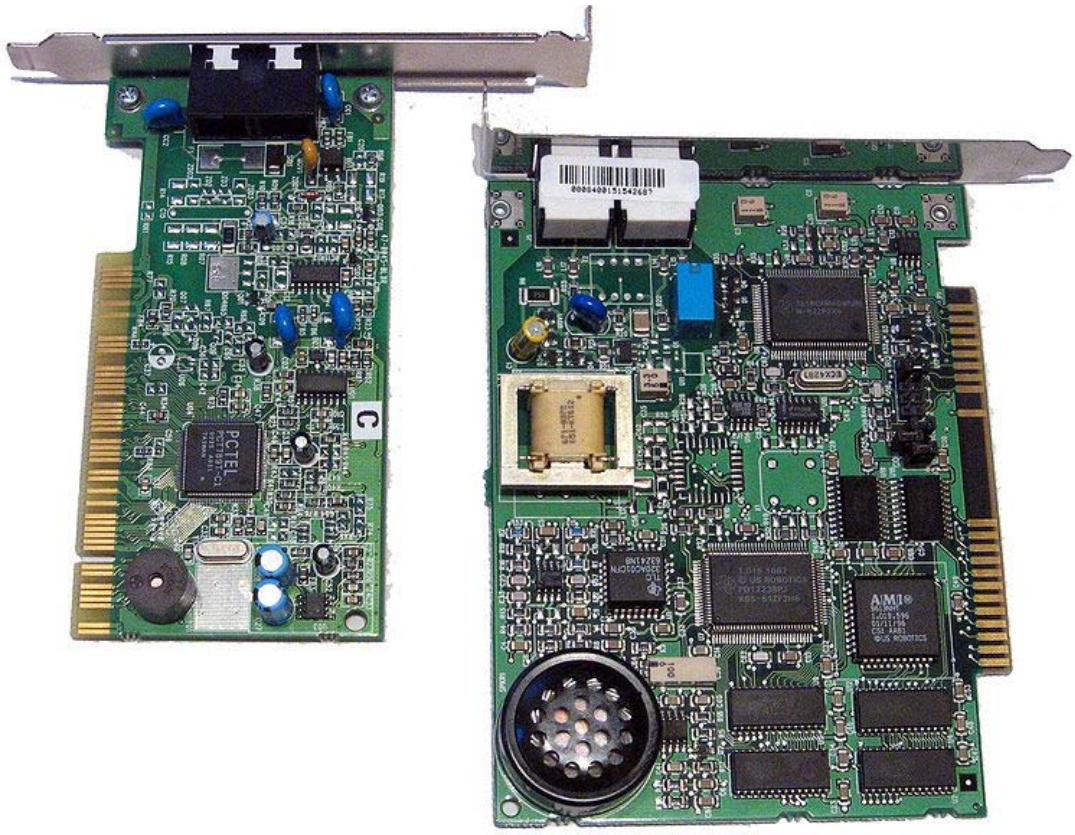
Prior to the Hayes *Smartmodem*, dial-up modems almost universally required a two-step process to activate a connection: first, the user had to manually dial the remote number on a standard phone handset, and then secondly, plug the handset into an acoustic coupler. Hardware add-ons, known simply as *dialers*, were used in special circumstances, and generally operated by emulating someone dialing a handset.

With the Smartmodem, the computer could dial the phone directly by sending the modem a command, thus eliminating the need for an associated phone instrument for dialing and the need for an acoustic coupler. The Smartmodem instead plugged directly into the phone line. This greatly simplified setup and operation. Terminal programs that maintained lists of phone numbers and sent the dialing commands became common.

The Smartmodem and its clones also aided the spread of bulletin board systems (BBSs). Modems had previously been typically either the call-only, acoustically coupled models used on the client side, or the much more expensive, answer-only models used on the server side. The Smartmodem could operate in either mode depending on the commands sent from the computer. There was now a low-cost server-side modem on the market, and the BBSs flourished.

Almost all modern modems can interoperate with fax machines. Digital faxes, introduced in the 1980s, are simply a particular 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 since has become largely universal.

**Softmodem (dumb modem)**




A PCI Winmodem/softmodem (on the left) next to a traditional ISA modem (on the right). Notice the less complex circuitry of the modem on the left.

A *Winmodem* or *softmodem* is a stripped-down modem that replaces tasks traditionally handled in hardware with software. In this case the modem is a simple interface designed to create voltage variations on the telephone line and to sample the line voltage levels (digital to analog and analog to digital converters). Softmodems are cheaper than traditional modems, since they have fewer hardware components. One downside is that the software generating and interpreting the modem tones is not simple (as most of the protocols are complex), and the performance of the computer as a whole often suffers when it is being used. For online gaming this can be a real concern. Another problem is lack of portability such that non-Windows operating systems (such as Linux) often do not have an equivalent driver to operate the modem.

## *Narrow-band/phone-line dialup modems*

A standard modem of today contains two functional parts: an analog section for generating the signals and operating the phone, and a digital section for setup and control. This functionality is often incorporated into a single chip nowadays, but the division remains in theory. In operation the modem can be in one of two modes, *data mode* in

which data is sent to and from the computer over the phone lines, and *command mode* in which the modem listens to the data from the computer for commands, and carries them out. A typical session consists of powering up the modem (often inside the computer itself) which automatically assumes command mode, then sending it the command for dialing a number. After the connection is established to the remote modem, the modem automatically goes into data mode, and the user can send and receive data. When the user is finished, the escape sequence, "+++" followed by a pause of about a second, may be sent to the modem to return it to command mode, then a command (e.g. "ATH") to hang up the phone is sent. Note that on many modem controllers it is possible to issue commands to disable the escape sequence so that it is not possible for data being exchanged to trigger the mode change inadvertently.

The commands themselves are typically from the Hayes command set, although that term is somewhat misleading. The original Hayes commands were useful for 300 bit/s operation only, and then extended for their 1,200 bit/s modems. Faster speeds required new commands, leading to a proliferation of command sets in the early 1990s. Things became considerably more standardized in the second half of the 1990s, when most modems were built from one of a very small number of chipsets. We call this the Hayes command set even today, although it has three or four times the numbers of commands as the actual standard.

## Increasing speeds (V.21, V.22, V.22bis)


A 2,400 bit/s modem for a laptop.

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 putting its 0s on 2,025 Hz and 1s on 2,225 Hz. These frequencies were chosen carefully, they are in the range that suffer minimum distortion on the phone system, and also 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 the similar frequencies as in the

300 bit/s systems, but slightly out of phase. By comparing the phase of the two signals, 1s and 0s could be pulled back out, for instance if the signals were 90 degrees out of phase, this represented two digits, *1, 0*, at 180 degrees it was *1, 1*. In this way each cycle of the signal represents two digits instead of one. 1,200 bit/s modems were, in effect, 600 symbols per second modems (600 baud modems) with 2 bits per symbol.

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 signalling was introduced in the U.S., and a slightly different one in Europe. By the late 1980s, most modems could support all of these standards and 2,400-bit/s operation was becoming common.

## Increasing speeds (one-way 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.

U.S. Robotics (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.

## 4,800 and 9,600 bit/s (V.27ter, V.32)

Echo cancellation was the next major advance in modem design. Local telephone lines use the same wires to send and receive, which results in a small amount of the outgoing signal bouncing back. This signal can confuse the modem, which was unable to distinguish between the echo and the signal from the remote modem. This was why earlier modems split the signal frequencies into 'answer' and 'originate'; the modem could

then ignore its own transmitting frequencies. 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 got around this problem. Measuring the echo delays and magnitudes allowed the modem to tell if the received signal was from itself or the remote modem, and create an equal and opposite signal to cancel its own. Modems were then able to send over the whole frequency spectrum in both directions at the same time, leading to the development of 4,800 and 9,600 bit/s modems.

Increases in speed have used increasingly complicated communications theory. 1,200 and 2,400 bit/s modems used the phase shift key (PSK) concept. This could transmit two or three bits per symbol. The next major advance encoded four bits into a combination of amplitude and phase, known as Quadrature Amplitude Modulation (QAM). Best visualized as a constellation diagram, the bits are mapped onto points on a graph with the x (real) and y (quadrature) coordinates transmitted over a single carrier.

The new V.27ter and V.32 standards were able to transmit 4 bits per symbol, at a rate of 1,200 or 2,400 baud, giving an effective bit rate of 4,800 or 9,600 bit/s. The carrier frequency was 1,650 Hz. For many years, most engineers considered this rate to be the limit of data communications over telephone networks.

### *Error correction and compression*

Operations at these speeds pushed the limits of the phone lines, resulting in high error rates. This led to the introduction of error-correction systems built into the modems, made most famous with Microcom's MNP systems. A string of MNP standards came out in the 1980s, each increasing the effective data rate by minimizing overhead, from about 75% theoretical maximum in MNP 1, to 95% in MNP 4. The new method called MNP 5 took this a step further, adding data compression to the system, thereby increasing the data rate above the modem's rating. Generally the user could expect an MNP5 modem to transfer at about 130% the normal data rate of the modem. Details of MNP were later released and became popular on a series of 2,400-bit/s modems, and ultimately led to the development of V.42 and V.42bis ITU standards. V.42 and V.42bis were non-compatible with MNP but were similar in concept: Error correction and compression.

Another common feature of these high-speed modems was the concept of fallback, or *speed hunting*, allowing them to talk to less-capable modems. During the call initiation the modem would play a series of signals into the line and wait for the remote modem to respond to them. They would start at high speeds and progressively get slower and slower until they heard an answer. 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 fallback 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 only 2,400 bit/s.

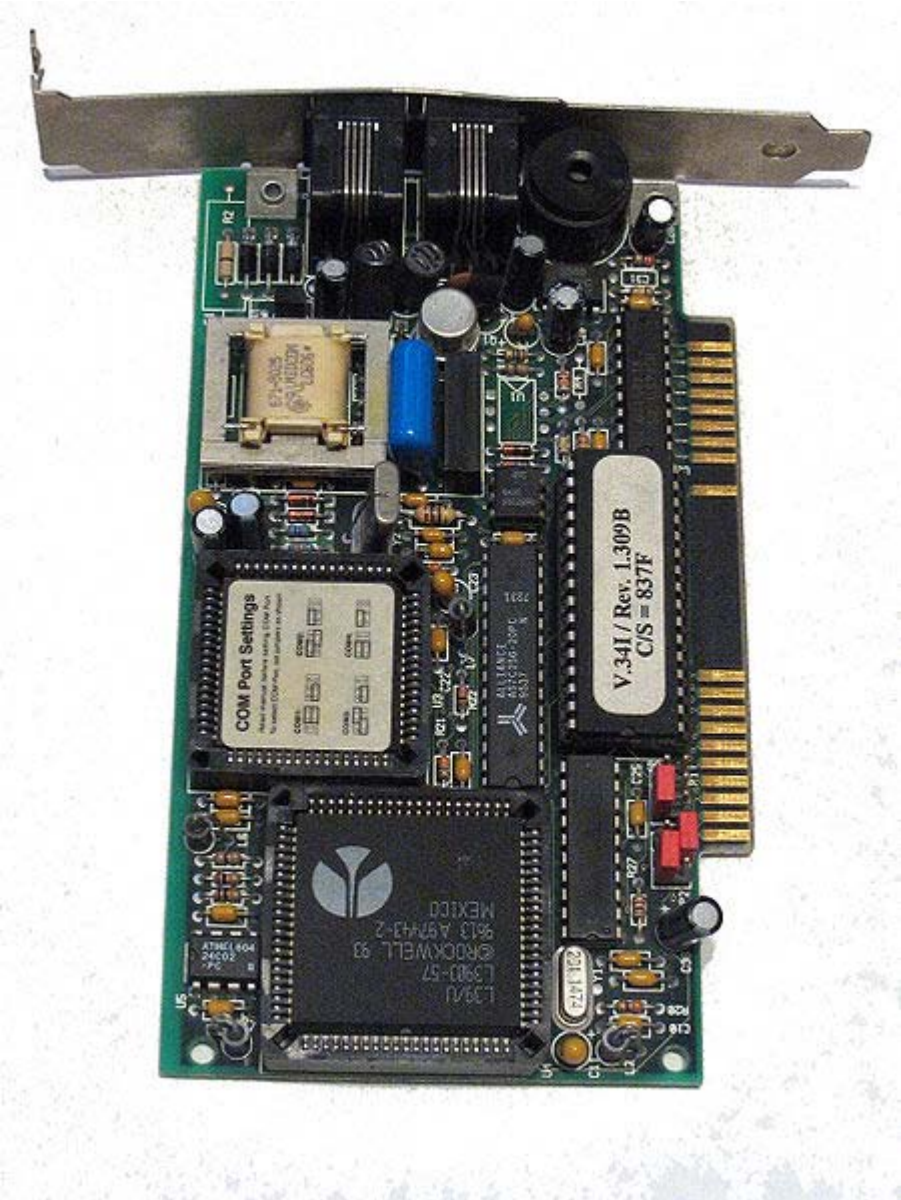
## Breaking the 9.6k barrier

In 1980, Gottfried Ungerboeck from IBM Zurich Research Laboratory applied powerful 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. Finally in 1982, he agreed to publish what is now a landmark paper in the theory of information coding. By applying powerful 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.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 (also known as V.32 terbo or *tertiary*), but neither non-standard modem sold well.

***V.34/28.8k and 33.6k***




An ISA modem manufactured to conform to the V.34 protocol.

Any interest in these systems 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.

Today, 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 4 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 $Bandwidth*log_2(1+P_u/P_n)$, with $P_u/P_n$ the (linear) signal-to-noise ratio. Narrowband phone lines have a bandwidth from 300-4000 Hz, so using $P_u/P_n=1000$ (SNR = 30dB): capacity is approximately 35 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. (DSL makes use of the bandwidth of traditional copper-wire twisted pairs between subscriber and the central office, which far exceeds that of analog voice circuitry.)

### *V.61/V.70 Analog/Digital Simultaneous Voice and Data*

The V.61 Standard introduced Analog Simultaneous Voice and Data (ASVD). This technology allowed users of v.61 modems to engage in point-to-point voice conversations with each other while their respective modems communicated.

In 1995, the first DSVD (Digital Simultaneous Voice and Data) modems became available to consumers, and the standard was ratified as v.70 by the International Telecommunication Union (ITU) in 1996.

Two DSVD modems can establish a completely digital link between each other over standard phone lines. Sometimes referred to as "the poor man's ISDN," and employing a similar technology, v.70 compatible modems allow for a maximum speed of 33.6 kbps between peers. By using a majority of the bandwidth for data and reserving part for voice transmission, DSVD modems allow users to pick up a telephone handset interfaced with the modem, and initiate a call to the other peer.

One practical use for this technology was realized by early two player video gamers, who could hold voice communication with each other while in game over the PSTN.

Advocates of DSVD envisioned whiteboard sharing and other practical applications for the standard, however, with advent of cheaper 56kbps analog modems intended for Internet connectivity, peer-to-peer data transmission over the PSTN became quickly irrelevant. Also, the standard was never expanded to allow for the making or receiving of arbitrary phone calls while the modem was in use, due to the cost of infrastructure upgrades to telephone companies, and the advent of ISDN and DSL technologies which effectively accomplished the same goal.

Today, Multi-Tech is the only known company to continue to support a v.70 compatible modem. While their device also offers v.92 at 56kbps, it remains significantly more expensive than comparable modems sans v.70 support.

## Using digital lines and PCM (V.90/92)

Modem bank at an ISP.

In the late 1990s Rockwell/Lucent and U.S. Robotics introduced new competing technologies based upon the digital transmission used in modern 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.

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. For example 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 to reconnect at a fast pace.

### Using compression to exceed 56k

Today'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*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.

## Compression by the ISP

As telephone-based 56k modems began losing popularity, some Internet service providers such as Netzero and Juno started using pre-compression to increase the throughput and maintain their customer base. As example, the Netscape ISP uses a compression program that squeezes images, text, and other objects at the modem server, just prior to sending them across the phone line. Certain content using lossy compression (e.g., images) may be recompressed (transcoded) using different parameters to the compression algorithm, making the transmitted content smaller but of lower quality. The server-side compression operates much more efficiently than the on-the-fly compression of V.44-enabled modems due to the fact that V.44 is a generalized compression algorithm whereas other compression techniques are application-specific (JPEG, MPEG, Vorbis, etc.). Typically Website text is compacted to 4% thus increasing effective throughput to approximately 1,300 kbit/s. The accelerator also pre-compresses Flash executables and images to approximately 30% and 12%, respectively.

The drawback of this approach is a loss in quality, where the GIF and JPEG images are lossy compressed, which causes the content to become pixelated and smeared. However the speed is dramatically improved such that Web pages load in less than 5 seconds, and the user can manually choose to view the uncompressed images at any time. The ISPs employing this approach advertise it as "surf 5× faster" or simply "accelerated dial-up".

### List of dialup speeds

Note that the values given are maximum values, and actual values may be slower under certain conditions (for example, noisy phone lines). A baud is one symbol per second; each symbol may encode one or more data bits.

| Connection | Bitrate (kbit/s) | Year Released |
|---|---|---|
| 110 baud Bell 101 modem | 0.1 | 1958 |
| 300 baud (Bell 103 or V.21) | 0.3 | 1962 |
| 1200 modem (1200 baud) (Bell 202) | 1.2 | |
| 1200 Modem (600 baud) (Bell 212A or V.22) | 1.2 | |
| 2400 Modem (600 baud) (V.22bis) | 2.4 | |
| 2400 Modem (1200 baud) (V.26bis) | 2.4 | |
| 4800 Modem (1600 baud) (V.27ter) | 4.8 | |
| 9600 Modem (2400 baud) (V.32) | 9.6 | |
| 14.4k Modem (2400 baud) (V.32bis) | 14.4 | |
| 28.8k Modem (3200 baud) (V.34) | 28.8 | |
| 33.6k Modem (3429 baud) (V.34) | 33.6 | |
| 56k Modem (8000/3429 baud) (V.90) | 56.0/33.6 | |
| 56k Modem (8000/8000 baud) (V.92) | 56.0/48.0 | |
| Bonding modem (two 56k modems)) (V.92) | 112.0/96.0 | |
| Hardware compression (variable) (V.90/V.42bis) | 56.0-220.0 | |
| Hardware compression (variable) (V.92/V.44) | 56.0-320.0 | |
| Server-side web compression (variable) (Netscape ISP) | 100.0-1,000.0 | |

## *Radio modems*

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, however signal attenuation

becomes a major problem at high data rates if a digital signal is used. By using a modem, a much larger amount of digital data can be transmitted through a single piece of 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.

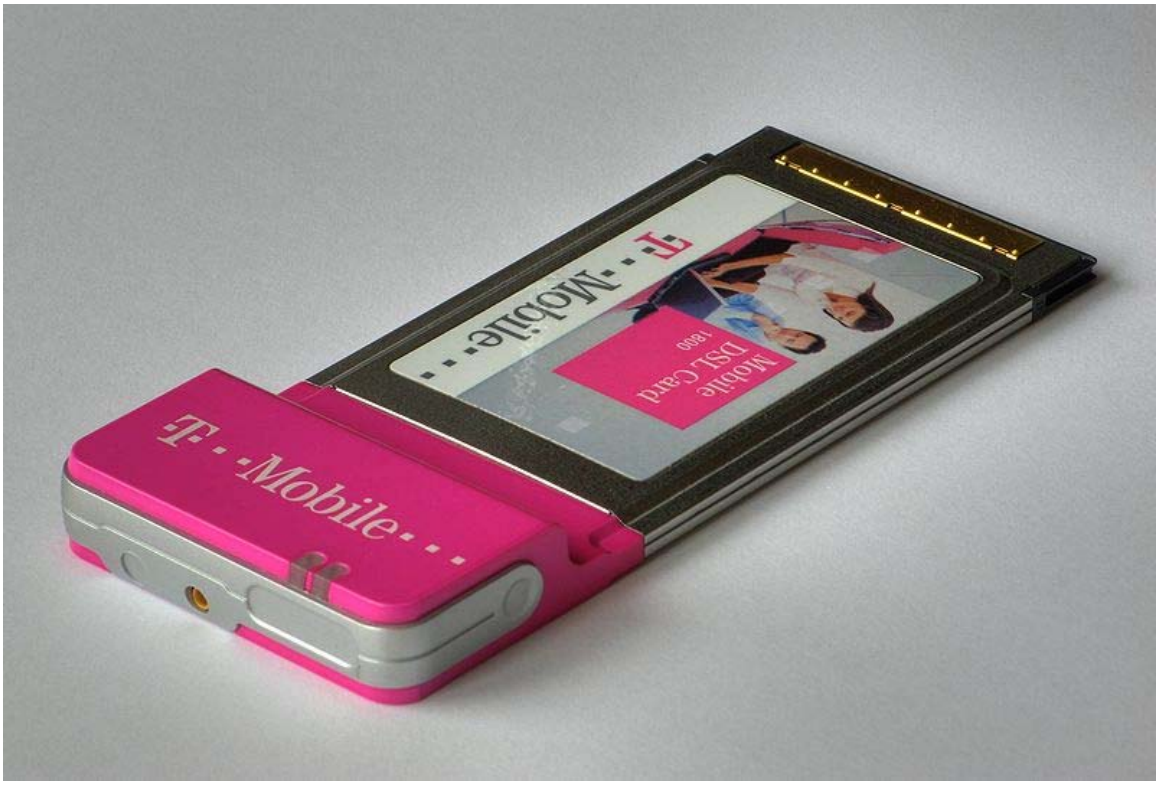
Smart modems come with a media access controller inside which prevents random data from colliding and resends data that is not correctly received. Smart modems typically require more bandwidth than transparent modems, and typically achieve higher data rates. The IEEE 802.11 standard defines a short range modulation scheme that is used on a large scale throughout the world.

## WiFi and WiMax

Wireless data modems are used in the WiFi and WiMax standards, operating at microwave frequencies.

WiFi is principally used in laptops for Internet connections (wireless access point) and wireless application protocol (WAP).

## *Mobile modems and routers*




T-Mobile Universal Mobile Telecommunications System PC Card modem


Huawei CDMA2000 Evolution-Data Optimized USB wireless modem

Modems which use a mobile telephone system (GPRS, UMTS, HSPA, EVDO, WiMax, etc.), are known as wireless modems (sometimes also called cellular modems). Wireless modems can be embedded inside a laptop or appliance or 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 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 per se, 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, or support multipoint to multipoint connections), while the modem is made for one connection.

Most of the 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.

## *Broadband*


DSL modem

ADSL modems, a more recent development, are not limited to the telephone's voiceband audio frequencies. Some ADSL modems use coded orthogonal frequency division modulation (DMT, for Discrete MultiTone; also called COFDM, for digital TV in much of the world).

Cable modems use a range of frequencies originally intended to carry RF television channels. Multiple cable modems attached to a single cable can use the same frequency band, using a low-level media access protocol to allow them to work together within the same channel. Typically, 'up' and 'down' signals are kept separate using frequency division multiple access.

New types of broadband modems are beginning to appear, such as doubleway satellite and power line modems.

Broadband modems should still be classed as modems, since they use complex waveforms to carry digital data. They are more advanced devices than traditional dial-up modems as they are capable of modulating/demodulating hundreds of channels simultaneously.

Many broadband modems include the functions of a router (with Ethernet and WiFi ports) and other features such as DHCP, NAT and firewall features.

When broadband technology was introduced, networking and routers were unfamiliar to consumers. However, many people knew what a modem was as most internet access was through dial-up. Due to this familiarity, companies started selling broadband modems using the familiar term *modem* rather than vaguer ones like *adapter* or *transceiver*, or even "bridge".

Many broadband modems must be configured in bridge mode before they can use a router.

## *Home networking*

Although the name *modem* is seldom used in this case, modems are also used for high-speed home networking applications, specially 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.

## *Deep-space telecommunications*

Many modern modems have their origin in deep space telecommunications systems of the 1960s.

Differences between deep space telecom modems and landline modems:

- digital modulation formats that have high doppler immunity are typically used
- waveform complexity tends to be low, typically binary phase shift keying
- error correction varies mission to mission, but is typically much stronger than most landline modems

## *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. This type of modem can be used as an FXO card for Private branch exchange systems (compare V.92).

## *Popularity*

A CEA study in 2006 found that dial-up Internet access is on a notable decline in the U.S. In 2000, dial-up Internet connections accounted for 74% of all U.S. residential Internet connections. The US demographic pattern for (dial-up modem users per capita) has been more or less mirrored in Canada and Australia for the past 20 years.

Dial-up modem use in the US had dropped to 60% by 2003, and in 2006 stood at 36%. Voiceband modems were once the most popular means of Internet access in the U.S., but with the advent of new ways of accessing the Internet, the traditional 56K modem is losing popularity.

Chapter 9

# Interplanetary Internet

The speed of light, illustrated here by a beam of light traveling from the Earth to the Moon, limits the speed at which Interplanetary Internet messages would be able to travel. In this example, it takes light 1.26 seconds to travel from the Earth to the Moon. Due to the vast distances involved, much longer delays are incurred than in the Earth-bound Internet.

The **Interplanetary Internet** (IPN) is a conceived computer network in space, consisting of a set of network nodes which can communicate with each other. Communication would be greatly delayed by the great interplanetary distances, so the IPN needs a new set of protocols and technology that are tolerant to large delays and errors. While the Internet as we know it tends to be a busy "network of networks" with high traffic, negligible delay and errors, and a wired backbone, the Interplanetary Internet is a store-and-forward "network of Internets" that is often disconnected, has a wireless backbone fraught with error-prone links and delays ranging to tens of minutes, even hours, even when there is a connection.

## *Development*

Space communication technology has steadily evolved from expensive, one-of-a-kind point-to-point architectures, to the re-use of technology on successive missions, to the development of standard protocols agreed upon by space agencies of many countries.

This last phase has gone on since 1982 through the efforts of the Consultative Committee for Space Data Systems (CCSDS), a body composed of the major space agencies of the world. It has 11 member agencies, 22 observer agencies, and over 100 industrial associates.

The evolution of space data system standards has gone on in parallel with the evolution of the Internet, with conceptual cross-pollination where fruitful, but largely as a separate evolution. Since the late 1990s, familiar Internet protocols and CCSDS space link protocols have integrated and converged in several ways, for example, the successful FTP file transfer to Earth-orbiting STRV-1b on January 2, 1996, which ran FTP over the CCSDS IPv4-like Space Communications Protocol Specifications (SCPS) protocols. Internet Protocol use without CCSDS has taken place on spacecraft, e.g., demonstrations on the UoSAT-12 satellite, and operationally on the Disaster Monitoring Constellation. Having reached the era where networking and IP on-board spacecraft have been shown to be feasible and reliable, a forward-looking study of the bigger picture was the next phase.


ICANN meeting, Los Angeles, USA, 2007. The marquee plays a humorous homage to the Ed Wood film *Plan 9 from Outer Space*, while namedropping Internet pioneer Vint Cerf.

The Interplanetary Internet study at NASA's Jet Propulsion Laboratory (JPL) was started by a team of scientists at JPL led by Vinton Cerf and Adrian Hooke. Cerf is one of the pioneers of the Internet on Earth, and currently holds the position of distinguished visiting scientist at JPL. Hooke is one of the directors of the CCSDS.

While IP-like SCPS protocols are feasible for short hops, such as ground station to orbiter, rover-to-lander, lander-to-orbiter, probe-to-flyby, and so on, delay-tolerant networking is needed to get information from one region of the solar system to another. It becomes apparent that the concept of a "region" is a natural architectural factoring of the InterPlanetary Internet.

A "region" is an area where the characteristics of communication are the same. Region characteristics include communications, security, the maintenance of resources, perhaps ownership, and other factors. The Interplanetary Internet is a "network of regional internets."

What is needed then, is a standard way to achieve end-to-end communication through multiple regions in a disconnected, variable-delay environment using a generalized suite of protocols. Examples of regions might include the terrestrial Internet as a region, a region on the surface of the moon or Mars, or a ground-to-orbit region.

The recognition of this requirement led to the concept of a "bundle" as a high-level way to address the generalized Store-and-Forward problem. Bundles are an area of new protocol development in the upper layers of the OSI model, above the Transport Layer with the goal of addressing the issue of bundling store-and-forward information so that it can reliably traverse radically dissimilar environments constituting a "network of regional internets."

Bundle Service Layering, implemented as the Bundling protocol suite for delay-tolerant networking, will provide general purpose delay-tolerant protocol services in support of a range of applications: custody transfer, segmentation and reassembly, end-to-end reliability, end-to-end security, and end-to-end routing among them. The Bundle Protocol was first tested in space on the UK-DMC satellite in 2008.

The *Deep Impact* mission

An example of one of these end-to-end applications flown on a space mission is CFDP, used on the comet mission, *Deep Impact*. CFDP is the CCSDS File Delivery Protocol an international standard for automatic, reliable file transfer in both directions. CFDP should not be confused with Coherent File Distribution Protocol, which unfortunately has the same acronym and is an IETF-documented experimental protocol for rapidly deploying files to multiple targets in a highly-networked environment.

In addition to reliably copying a file from one entity (i. e., a spacecraft or ground station) to another entity, the CCSDS CFDP has the capability to reliably transmit arbitrary small messages defined by the user, in the metadata accompanying the file, and to reliably transmit commands relating to file system management that are to be executed

automatically on the remote end-point entity (i. e., a spacecraft) upon successful reception of a file.

## *Implementation*

The dormant InterPlanetary Internet Special Interest Group of the Internet Society has worked on defining protocols and standards that would make the IPN possible. The Delay-Tolerant Networking Research Group (DTNRG) is the primary group researching Delay-tolerant networking. Additional research efforts focus on various uses of the new technology.

As of 2005, NASA has canceled plans to launch the Mars Telecommunications Orbiter in September 2009; it had the goal of supporting future missions to Mars and would have functioned as a possible first definitive Internet hub around another planetary body.

NASA JPL continued to test the DTN protocol with their Deep Impact Networking (DINET) experiment onboard the *Deep Impact*/EPOXI spacecraft in October, 2008.

In May 2009, DTN was deployed to a payload onboard the ISS. NASA and BioServe Space Technologies, a research group at the University of Colorado, have been continuously testing DTN on two Commercial Generic Bioprocessing Apparatus (CGBA) payloads. CGBA-4 and CGBA-5 serve as computational and communications platforms which are remotely controlled from BioServe's Payload Operations Control Center (POCC) in Boulder, CO. These initial experiments provide insight into future missions where DTN will enable the extension of networks into deep space to explore other planets and solar system points of interest. Seen as necessary for space exploration, DTN enables timeliness of data return from operating assets which results in reduced risk and cost, increased crew safety, and improved operational awareness and science return for NASA and additional space agencies.

DTN has several major arenas of application, in addition to the Interplanetary Internet, which include sensor networks, military and tactical communications, disaster recovery, hostile environments, mobile devices and remote outposts. As an example of a remote outpost, imagine an isolated Arctic village, or a faraway island, with electricity, one or more computers, but no communication connectivity. With the addition of a simple wireless hotspot in the village, plus DTN-enabled devices on, say, dog sleds or fishing boats and have their requests forwarded to the nearest networked location on the sled's or boat's next visit, and get the replies on its return.

Chapter 10

# ARINC 825

## *ARINC Specification 825 - The General Standardization of CAN for Airborne Use*

Controller Area Network (CAN) increasingly found its way into aerospace applications because of its cost effective and efficient networking capability for systems employing the Line-replaceable unit (LRU) concept to share data across a common media. The ability of CAN to transmit data, across a shared shielded twisted pair cable, has advantages in terms of weight savings at the aircraft integration level. Additionally, the CAN physical layer protocol specification provides error recovery and protection mechanisms that make this data bus standard attractive to aviation applications. Newer commercial air transport aircraft like the Airbus A380 or the Boeing 787 already accommodate between 50 and 250 CAN networks for all sorts of functions including flight deck systems, engine control and flight control systems. In an effort to provide a common standard for the use of CAN in commercial air transport, Airbus and Boeing initiated the CAN Technical Working Group of the Airlines Electronic Engineering Committee to define the ARINC specification 825. The target of ARINC 825 is to ensure interoperability and to simplify interoperation of CAN subsystems with other airborne networks for all classes of aircraft including the commercial air transport segment. The CAN Technical Working Group initially consisted of members from Airbus, Boeing, Rockwell Collins, GE Aerospace and Stock Flight Systems () and published the ARINC 825 specification in November, 2007 with supplement 1 being released by May, 2010. The ARINC specification 825 was influenced by the CANaerospace standard to a high degree.

## *Role of CAN in Commercial Air Transport and General Aviation Aircraft*

Current commercial air transport aircraft system architectures have incorporated CAN as an ancillary subsystem bus to ARINC Specification 664, Part 7 (AFDX), networked Integrated Modular Avionics (IMA) architectures. For these aircraft, CAN has been used to link sensors, actuators and other types of avionics devices that typically require low to

medium data transmission volumes during operation. In this role, CAN complements higher capacity networks that support systems controlling the flight deck information flow and presentation. In contrary, General Aviation system architectures employ CAN as one of the major avionics buses or even as the avionics backbone network. In this role CAN may have to fulfill all requirements of a flight safety critical network. The ARINC Specification 825 enhances CAN to create a network that embraces both philosophies. It may be used as a primary or ancillary avionics network and was designed to meet the following requirements:

- **Easy connections of local CAN networks to other airplane networks.**
- **Minimal cost of implementation and cost of change over time.**
- **Maximum interoperability and interchangeability of CAN connected LRUs.**
- **Configuration flexibility: easy addition, deletion, and modification of bus nodes, without undue impact onto other LRUs.**
- **Simplified system and network boundary crossing for both parametric and block data transfers.**
- **Integrated error detection and error signaling.**
- **Support for system level functions such as on-board data load and airplane health management.**

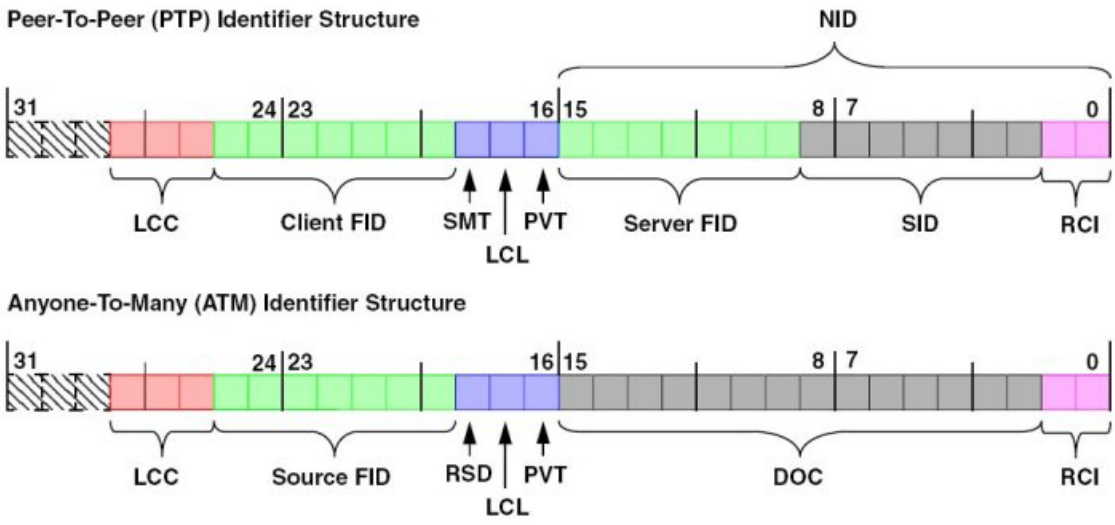
## *Physical Interface*

To ensure interoperability and reliable communication, ARINC 825 specifies the electrical characteristics, bus transceiver requirements and data rates with the corresponding tolerances based on ISO 11898. The bit timing calculation (baud rate accuracy, sample point definition) and robustness to electromagnetic interference are given special emphasis. Also addressed within ARINC 825 are CAN connector and wiring considerations. The data rates supported by ARINC 825 are 1000 kbit/s, 500 kbit/s, 250 kbit/s, 125 kbit/s and 83.333 kbit/s.

## *Identifier Usage and Communication Layers*

ARINC 825 is entirely based on CAN 2.0B using extended frames (29-bit identifiers) which provide an adequate number of bits to divide the identifier into several sub-fields. These sub-fields are a key issue in employing the identifier bits not only for the data object identification and transmission prioritization inherent to CAN but also for the purpose of creating a standardized application layer. CAN communication using 11-bit identifiers may coexist on an ARINC 825 bus if it is free of potential deadlock scenarios caused by single source bus masters.

The communication mechanisms of ARINC 825 are derived from the corresponding CANaerospace mechanisms. Just like CANaerospace, ARINC 825 defines additional ISO layer 3, 4 and 6 functions to support logical communication channels, one-to-many/peer-to-peer communication and station addressing. To accomplish this, the 29-Bit CAN identifier is given a special structure for ARINC 825 (see Figure 1). Logical Communication Channels (LCCs) provide these independent layers of communication (see Figure 2).




| Field | Description |
|---|---|
| LCC | Logical Communication Channel |
| FID | Aircraft Function ID |
| RSD | Reserved |
| SMT | Service Message Type |
| LCL | Local Bus Only |

| Field | Description |
|---|---|
| PVT | Private Data |
| SID | Server ID |
| RCI | Redundancy Channel ID |
| NID | Node ID |
| DOC | Data Object Code |

**Figure 1: ARINC 825 CAN Identifier Structures**

| Channel Number | Channel Acronym | Communication Type | Description | LCC Bits | Message Priority |
|---|---|---|---|---|---|
| 0 | EEC | ATM | Exception Event Channel | 000 | Highest |
| 1 | | | Reserved | 001 | |
| 2 | NOC | ATM | Normal Operation Channel | 010 | |
| 3 | | | Reserved | 011 | |
| 4 | NSC | PTP | Node Service Channel | 100 | |
| 5 | UDC | ATM/PTP | User-defined Channel | 101 | |
| 6 | TMC | PTP | Test and Maintenance Channel | 110 | |
| 7 | FMC | ATM/PTP | CAN Base Frame Migration Channel | 111 | Lowest |

Figure 2: ARINC 825 Logical Communication Channel Assignment

## *Interoperability*

To support interoperability in airborne systems, ARINC 825 includes:

- **Data Endian definition (Big Endian exclusively)**
- **Data Type definition (Boolean, Integer, Floating-Point, ....)**
- **Aeronautical Axis System and Sign Convention (ISO1151/EN9300)**
- **Engineering Unit definitions (m, kg, ....)**
- **Aircraft Function definition (Flight State, Air Data, ....)**

The aircraft function definitions used to identify source and destination of messages are derived from the Air Transport Association (ATA) aircraft system chapters. This helps system engineers to assign the proper functions for their systems based on definitions well known in aeronautics since decades.

## *Bandwidth Management*

ARINC 825 adopted the CANaerospace bandwidth management concept known as "Time Triggered Bus Scheduling". This concept provides a means of computing the bus load based on the number of messages in a network segment and adjusting their transmission rates. Bandwidth management minimizes peak load scenarios and jitter caused by the CAN bus arbitration. Applying this concept, it can be demonstrated that ARINC 825 networks behave predictably and are able to fulfill the requirements for flight safety critical systems. For ensuring this under fault conditions the system designer has to define the behaviour under these conditions (such as high occurrence of error frames and avoidance of priority inversion) .

ARINC 825 may be used for systems classified up to Design Assurance Level (DAL) A if the effect of the loss of one bus does not present a hazard exceeding the classification "major". Figure 3 shows an example of two ARINC 825 nodes operating in accordance with the Time Triggered Bus Scheduling concept.

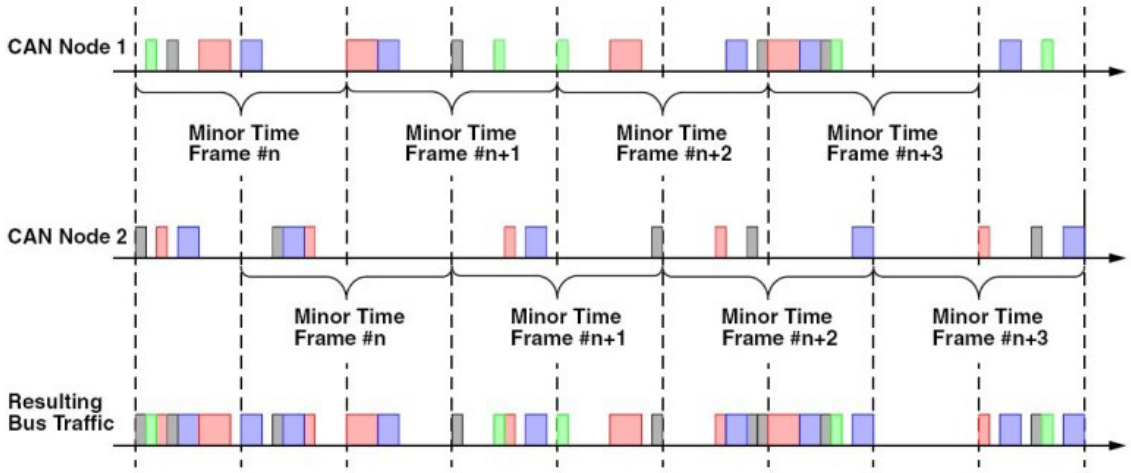



Figure 3: ARINC 825 Bandwidth Management

## Communication Profile Database

ARINC 825 uses a communication profile database for the description of integrated networks. A communication profile is created for each LRU in a human readable file format, since supplement 1 based on XML 1.0. The combination of all LRU communication profiles for a given network describes the entire bus traffic and provides a valuable means for specification and verification of ARINC 825 networks. An analysis of the communication profile database allows to detect potential network problems at an early stage. ARINC 825 test tools must be able to read the communication profile database and interpret network data accordingly.

## Gateways between ARINC 825 and other Networks

Commercial air transport aircraft Integrated Modular Avionics system architectures use multiple networks with different characteristics which have to exchange data with each other using gateways. Typically, bandwidth and communication principles of the involved networks differ widely. To support the design of gateways between CAN and other networks, ARINC 825 specifies a gateway model and provides substantial information about protocol conversion, bandwidth management, data buffering and fault isolation.

## Design Guidelines

The ARINC specification 825 contains a design guidelines section that helps system engineers and CAN LRU designers to implement ARINC 825 properly and in a

certifiable manner. This section is intended to document industry experience that led to the decisions in the ARINC Specification 825. The guidelines are general network design criteria to be considered when designing an ARINC 825 network; they are not requirements but rather the recommendations to avoid potential design traps a network designer may encounter.

## *Outlook*

The consistency and integrity of the ARINC specification 825 was continuously verified during the standardization process using a reference hardware/software system . The Airlines Electronic Engineering Committee decided that all future ARINC specifications using CAN (i.e. the ARINC 826 Data Load and ARINC 812 Galley Insert Communication Standards) shall be based on ARINC 825. Airbus Technical Design Directives already specify ARINC 825 for many systems of the new Airbus A350. CANaerospace continues to coexist with ARINC 825 as the "11-bit identifier alternative" and provides enhanced ARINC 825 compatibility starting with revision 1.8.