Computer Networking and Management

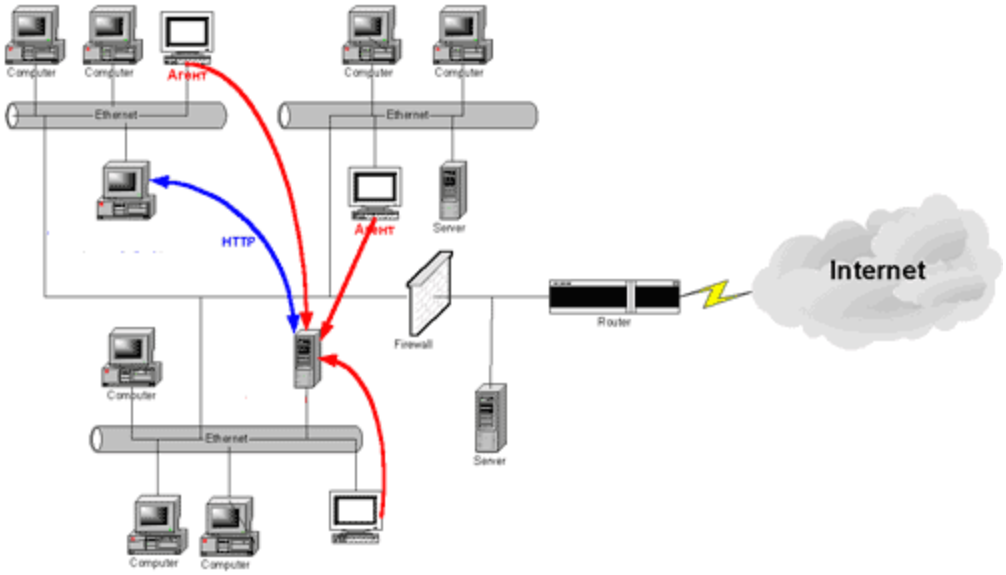
Lesson 1 - Computer Networks and Internet - Overview

Introduction | What is the Internet? | What is a protocol? | The Network Edge | The Network Core | Access Networks | Physical Media | Delay and Loss in Packet-Switched Networks | Protocol Layers and Their Service Models | Internet History

Lesson Outline

GOTO TOP

Introduction



This lesson provides a broad overview of the Computer Networking and the Internet. The lesson begins with an overview of the Internet and of networking protocols, introducing several key terms and concepts.

We examine the 'edge' of a computer network, looking at the end systems and applications, and at the transport service provided to applications running of the end systems

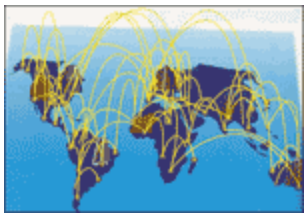
We also examine the 'core' of a computer network, examining the links and switches that transport data. We then take a broader view of networking. From a performance standpoint, we study the causes of packet delay and loss in computer network. We identify key architectural principles in networking, including layering and service models. We provide brief introduction history of computer networking.

Finally, we provide a brief overview of ATM, a networking technology that provides an important contrast with Internet technologies.

GOTO TOP

What is the Internet?

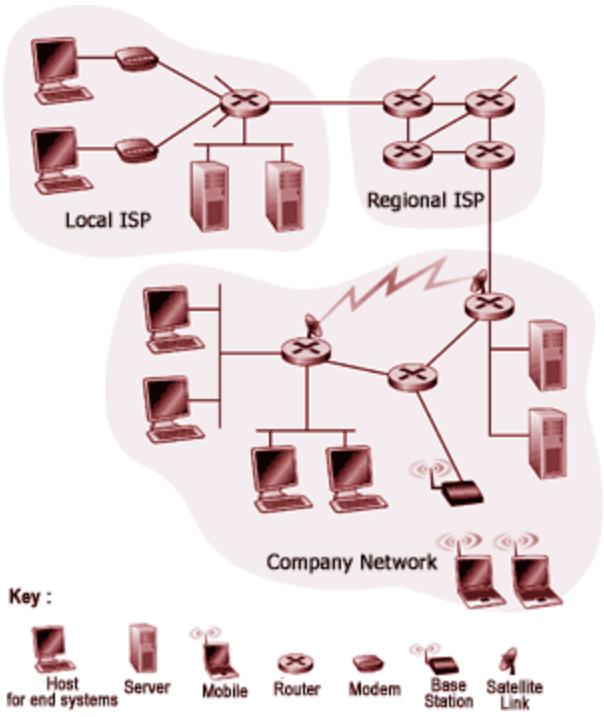
Here we use the public Internet, a specific computer network, as our principle vehicle for discussing computer networking protocols. But what is the Internet?



We would like to be able to give you a one-sentence definition of the Internet – a definition that you can take home and share with your family and friends. Alas, the Internet is very complex, both in terms of its hardware and software components, as well as in the services it provides.

GOTO TOP

What is the Internet: ‘Nuts and Bolts’ View



Instead of giving a one sentence definition, let us try a more descriptive approach. There are a couple of ways to do this. One way is to describe the nuts and bolts of the Internet, that is, the basic **hardware** and **software** components that make up the Internet. Another way is to describe the Internet in terms of **a networking infrastructure that provides services to distributed applications.**

Cool Internet Appliances

LG's Internet Microwave
http://www.lge.com/products/homenetwork/internetproduct/microwaveoven/microwaveoven.jsp

Qubit Touch Screen Tablet
http://www.x-home.com/e/e43.html

JCC's iBOX-2 with Geode and Linux inside
http://www.linuxdevices.com/news/NS4653311319.html

Digital Photo Receiver
http://www.ceiva.com

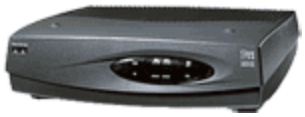
The public internet is a worldwide computer network, that is, a network that interconnects millions of computing devices throughout the world. Most of these computing devices are traditional desktop PCs, Unix-based workstations, and so called servers that store and transmit information such as Web (WWW) pages and e-mail

messages. Increasingly, non-traditional computing devices such as Web TVs, mobile computers, pagers, and toasters are being connected to the Internet.

In the Internet jargon, all of these devices are called hosts or end systems. The Internet applications, with which many of us are familiar, such as the Web and e-mail, are network application programs that run on such end systems.

End systems, as well as most other 'pieces' of the Internet, run protocols that control the sending and receiving of information within the Internet. **TCP (Transmission Control Protocol)** and **IP (Internet Protocol)** are two of the most important protocols in the Internet. The Internet's principal protocols are collectively known as TCP/IP.

End systems are connected together by communication links. Links are made up of different types of physical media, including coaxial cable, copper wire, fibre optics, and radio spectrum. Different links can transmit data at different rates. The link transmission rate is often called the link bandwidth and is typically measured in bits/second.



Usually, end systems are not directly attached to each other via a single communication link. Instead, they are indirectly connected to each other through intermediate **switching devices** known as **routers**. A router takes information arriving on one of its incoming communication links and then forwards that information on one of its outgoing communication links. The IP protocol specifies the format of the information that is sent and received among routers and end systems. The path that transmitted information takes from the sending end system, through a series of communications links and routers, to the receiving end system is known as a route or path through the network.

Rather than provide a dedicated path between communicating end systems, **the Internet uses a technique known as packet switching** that allows multiple communicating end systems to share a path, or parts of a path, at the same time. The earliest ancestors of the Internet were the first packet-switched networks.

The Internet is really a network of networks. That is, the Internet is an interconnected set of privately and publicly owned and managed networks. Any network connected to the Internet must run the IP protocol and conform to certain naming and addressing conventions. Other than these few constraints, however, a network operator can configure and run its network (that is, its little piece of Internet) however it chooses. Because of the universal use of the IP protocol in the Internet, the IP protocol is sometimes referred to as the Internet dial tone.

The topology of the Internet, that is, the structure of the interconnection among the various pieces of the internet, is loosely hierarchical. Roughly speaking, from bottom-to-top, the hierarchy consists of end systems connected to local Internet Service Providers (ISPs) through access networks. An access network may be a so-called local-area network within a company or university, a dial telephone line with a modem, or a high-speed cable-based or phone-based access network. Local ISPs are in turn connected to regional ISPs, which are in turn connected to national and international ISPs. The national and international ISPs are connected together at the highest tier in the hierarchy. New tiers and branches (that is, new networks, and new networks of networks) can be added.

At the technical and developmental level, the Internet is made possible through creation, testing, and implementation of Internet standards. These standards are developed by the Internet Engineering Task Force (IETF).

Things to Remember:

What is the Internet?

millions of connected computing devices: *hosts*, *end-systems*

- PCs,workstations, servers
- PDAs phones, toasters, running *network apps*

communication links

- fiber, copper, radio, satellite
- transmission rate = ***bandwidth***

routers: forward packets (chunks of data)

Things to Remember:

What is the Internet?

protocols control sending, receiving of msgs
e.g., TCP, IP, HTTP, FTP, PPP

Internet: "network of networks"

- loosely hierarchical
- public Internet versus private intranet

Internet standards

- RFC: Request for comments
- IETF: Internet Engineering Task Force

The IETF standards documents are called Request For Comments (RFCs). RFCs started out as general request for comments (hence the name) to resolve architecture problems that faced the precursor to the Internet. RFCs, though not formally standards, have evolved to the point where they are cited as such. RFCs tend to be quite technical and detailed. They define protocols such as TCP, IP, HTTP (for the web), and SMTP (for open-standards e-mail). There are more than 2,000 different RFCs.

The public Internet is the network that one typically refers to as the Internet. There are also many private networks, such as certain corporate and government networks, whose hosts are not accessible from (that is, they cannot exchange messages with) hosts outside of that private network. These private networks are often referred to as intranets, as they often use the same Internet technology (for example, the same types of host, routers, links, protocols, and standards) as the public Internet.

The preceding discussion has identified many of the pieces that make up the Internet.

Let us now leave the nuts-and-bolts description and take a more abstract service-oriented view.

GOTO TOP

What is the Internet: A Service View

The Internet allows distributed applications running on its end systems to exchange data with each other. These applications include remote login, file transfer, electronic mail, audio and video streaming, real-time audio and video conferencing, distributed games, the World Wide Web, and much, much more.

It is worth emphasizing that the Web is not a separate network but rather just one of many distributed applications that use the communication services provided by the Internet. The Web could also run over a network besides the Internet. One reason that the Internet is the communication medium of choice for the Web, however, is that no other existing packet switched network connects more than 100 million computers together and has over 350 million users.

> **Cyberspace** [Gibson]:
> "a consensual hallucination experienced daily by billions of operators, in every nation, ..."

The Internet provides two services to its distributed applications: a connection-oriented service and a connectionless oriented service.

Loosely speaking, connection-oriented service guarantees that data transmitted from a sender to a receiver will eventually be delivered to the receiver in order and its entirety.
Connectionless service does not make any guarantees about eventual delivery.

Typically, a distributed application makes use of one or the other of these two services and not both.

Currently, the Internet does not provide a service that makes promises about how long it will take to deliver the data from sender to receiver. Also, except for increasing your access bit rate to your Internet service provider, you currently cannot obtain better service (for example, shorter delays) by paying more.

Our second description of the Internet – in terms of the services it provides to distributed applications – is a non-traditional, but important, one. Increasingly, advances in the nuts-and-bolts components of the Internet are being driven by the needs of new applications. So it is important to keep in mind that the Internet is an infrastructure in which new applications are being constantly invented and deployed.

We have given two descriptions of the Internet, one in terms of its hardware and software components, the other in terms of the services it provides to distributed applications.

Things to Remember:

Communication infrastructure enables distributed applications:

- Web
- email
- games
- e-commerce
- database
- voting
- file (MP3) sharing

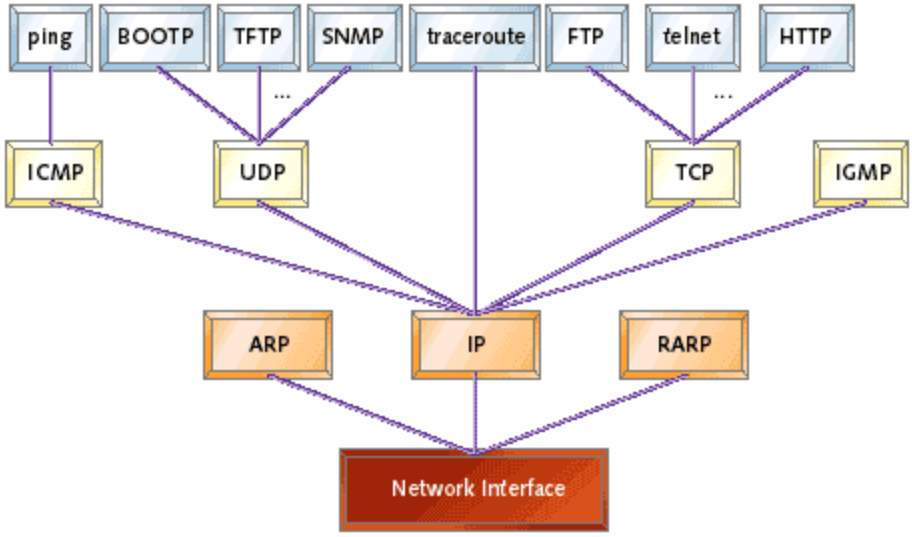
Communication services provided to apps:

- connectionless
- connection-oriented

GOTO TOP

What is a Protocol?

Now that we have got a bit of a feel for what the Internet is, let us consider another important buzzword in computer networking – protocol.



What is a protocol? What does a protocol do? How would you recognize a protocol if you met one?

human protocols:
"what's the time?"
"I have a question"
introductions

… specific msgs sent
… specific actions taken when msgs received, or other events

network protocols:
machines rather than humans
all communication activity in Internet governed by protocols

protocols define format, order of msgs sent and received among network entities, and actions taken on msg transmission, receipt

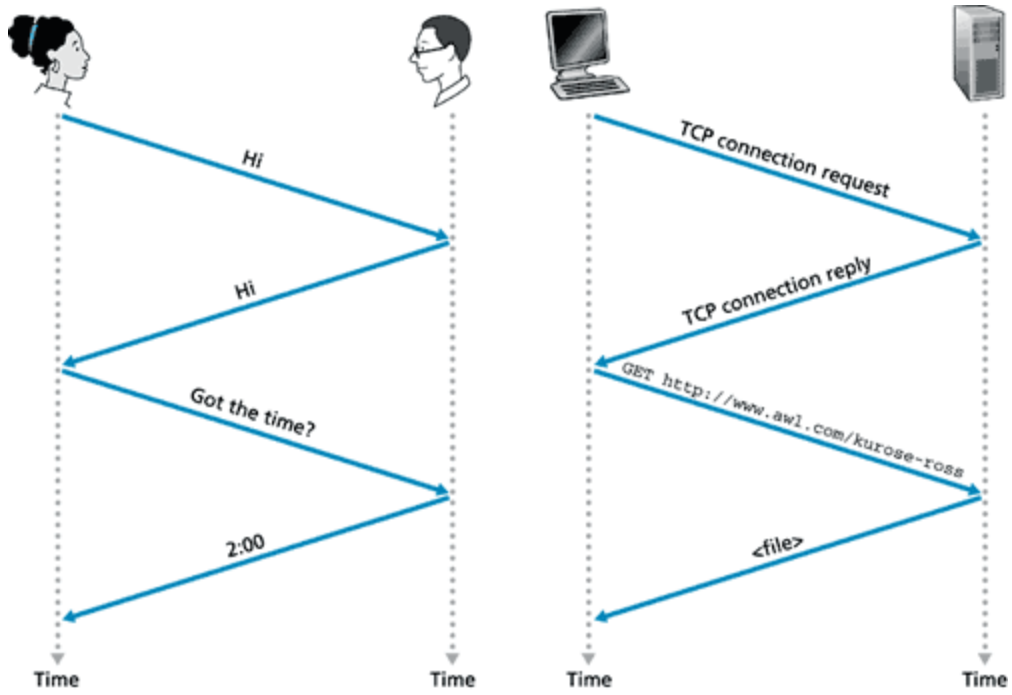
GOTO TOP

A Human Analogy

It is probably easiest to understand the notion of a computer network protocol by first considering some human analogies, since we humans execute protocols all of the time. Consider what you do when you ask someone for the time of day.

A typical exchange is shown in the following diagram. Human protocol dictates that one first offers a greeting (the first "Hi" in Figure) to initiate communication with someone else. The typical response to a "HI" message (at least outside of New York City) is a returned "Hi" message. Implicitly, one takes a cordial "Hi" response as an indication that one can proceed ahead and ask for the time of day. A different response to the initial "Hi" (such as "Don't bother me!" or "I don't speak English," or an unprintable reply that one might receive in New York City) might indicate an unwillingness or inability to communicate.

a human protocol and a computer network protocol:



In this case, the human protocol would be to not ask for the time of day. Sometimes one gets no response at all to a question, in which case one typically gives up asking that person for the time.

Note that in our human protocol, there are specific messages we send, and specific actions we take in response to the received reply messages or other events (such as no reply within some given amount of time). Clearly transmitted and received messages, and actions taken when these messages are sent or received or other events occur, play a central role in human protocol.

If people run different protocols (for example, if one person has manners but the other does not, or if one understands the concept of time and the other does not) the protocols do not interoperate and no useful work can be accomplished. The same is true in networking – it takes two (or more) communicating entities running the same protocol in order to accomplish a task.

GOTO TOP

A Human Protocol and a Computer Network Protocol

Let us consider a second human analogy. Suppose you are in a college class (a computer networking and management class, for example!). The teacher is droning on about protocols and you are confused.

The teacher stops to ask, "Are there any questions?" (a message that is transmitted to, and received by, all students who are not sleeping!). You raise your hand (transmitting an implicit message to the teacher).

Your teacher acknowledges you with a smile, saying "Yes. .." (a transmitted message encouraging you to ask your question -teachers love to be asked questions) and you then ask your question (that is, transmit your message to your teacher).

Your teacher hears your question (receives your question message) and answers (transmits a reply to you). Once again, we see that the transmission and receipt of messages, and a set of conventional actions taken when these messages are sent and received, are at the heart of this question-and-answer protocol.

GOTO TOP

Network Protocols

A network protocol is similar to a human protocol, except that the entities exchanging messages and taking

actions are hardware or software components of a computer network. All activity in the Internet that involves two or more communicating remote entities is governed by a protocol.

Protocols in routers determine a packet's path from source to destination; hardware - implemented protocols in the network interface cards of two physically connected computers control the flow of bits on the 'wire' between the two computers; a congestion - control protocol controls the rate at which packets are transmitted between sender and receiver.

Protocols are running everywhere in the Internet, and consequently much of this module is about computer network protocols.

As an example of a computer network protocol with which you are probably familiar, consider what happens when you make a request to a Web server, that is, when you type in the URL of a Web page into your Web browser.

- First, your computer will send a 'connection request' message to the Web server and wait for a reply. The Web server will eventually receive your connection request message and return a 'connection reply' message.
- Knowing that it is now OK to request the Web document, your computer then sends the name of the Web page it wants to fetch from that Web server in a 'get' message.
- Finally, the Web server returns the contents of the Web document to your computer.

Given the human and networking examples above, the exchange of messages and the actions taken when these messages are sent and received are the key defining elements of a protocol:

A protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.

The Internet and computer networks in general, make extensive use of protocols. Different protocols are used to accomplish different communication tasks.

GOTO TOP

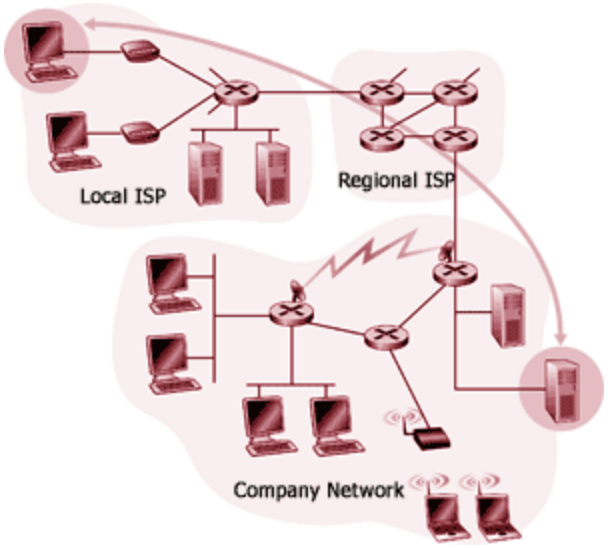
A closer look at network structure

- Network edge:
  - applications and hosts
- Network core:
  - routers
  - network of networks
- Access networks, physical media:
  - communication links

In the previous sections we presented a high-level description of the Internet and networking protocols. We are now going to delve a bit more deeply into the components of the Internet. We begin in this section at the edge of network and look at the components with which we are most familiar -the computers (for example, PCs and workstations) that we use on a daily basis. In the next section we will move from the network edge to the network core and examine switching and routing in computer networks. Then we will discuss the actual physical links that carry the signals sent between the computers and the switches.

GOTO TOP

The Network Edge



GOTO TOP

End Systems, Clients, and Servers

In computer networking jargon, the computers that we use on a daily basis are often referred to as hosts or end systems. They are referred to as hosts because they host (run) application-level programs such as a Web browser or server program, or an e-mail program. They are also referred to as end systems because they sit at the edge of the Internet, as shown in Visual 10. Throughout this module we will use the terms hosts and end systems interchangeably; that is, host = end system.

Things to Remember:

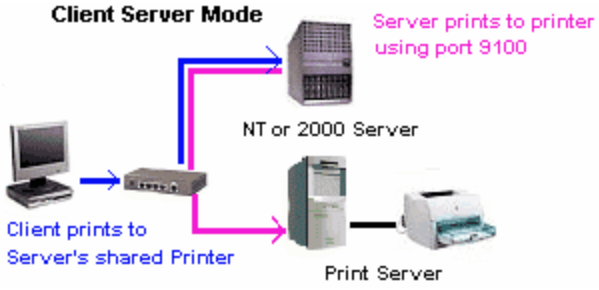
End systems (hosts):

- run application programs
- e.g., WWW, email
- at "edge of network"

GOTO TOP

End-System Interaction

Hosts are sometimes further divided into two categories: clients and servers. Informally, clients often tend to be desktop PCs or workstations, whereas servers are more powerful machines. But there is a more precise meaning of a client and a server in computer networking.



In the so-called client/server model, a client program running on one end system requests and receives information from a server running on another end system. This client/server model is undoubtedly the most prevalent structure for Internet applications.

The Web, e-mail, file transfer, remote login (for example, Telnet), newsgroups, and many other popular applications adopt the client/server model. Since a client typically runs on one computer and the server runs on another computer, client/server Internet applications are, by definition, distributed applications. The client and the server interact with each other by communicating (that is, sending each other message) over the Internet.

At this level of abstraction, the routers, links and other 'pieces' of the Internet serve as a 'black box' that transfers messages between the distributed,

Things to Remember:

Client/server model:

- client host requests, receives service from server
- e.g. Web browser/server; email client/server

Peer-peer model:

- host interaction symmetric
- e.g.: Gnutella, KaZaA

communicating components of an Internet application.

Computers (for example, a PC or a workstation), operating as clients and servers, are the most prevalent type of end system. However, an increasing number of alternative devices, such as so-called network computers and thin clients, Web TV s and set top boxes, digital cameras, etc. are being attached to the Internet as end systems.

GOTO TOP

Connection less and Connection-Oriented Services

We have seen that end systems exchange messages with each other according to an application-level protocol in order to accomplish some task. The links, routers, and other pieces of the Internet provide the means to transport these messages between the end- system applications. But what are the characteristics of the communication services that are provided? The Internet, and more generally TCP/IP networks, provides two types of services to its applications: **connection less service** and **connection-oriented service**.

A developer creating an Internet application (for example, an e-mail application, a file transfer application, a Web application, or an Internet phone application) must program the application to use one of these two services.

GOTO TOP

Connection-Oriented Service

When an application uses the connection-oriented service, the client and the server (residing in different end systems) send control packets to each other before sending packets with real data (such as e-mail messages). This so-called handshaking procedure alerts the client and server, allowing them to prepare for an onslaught of packets. It is interesting to note that this initial handshaking procedure is similar to the protocol used in human interaction.

The exchange of "Hi's" we saw is an example of a human 'handshaking protocol' (even though handshaking is not literally taking place between the two people). The two TCP messages that are exchanged as part of the WWW interaction detailed in the above visual are two of the three messages exchanged when TCP sets up a connection between a sender and receiver. The third TCP message (not shown) that forms the final part of the TCP three-way handshake is contained in the get message shown in the above diagram.

Once the handshaking procedure is finished, a connection is said to be established between the two end systems. But the two end systems are connected in a very loose manner, hence the terminology connection-oriented. In particular, only the end systems themselves are aware of this connection; the packet switches (that is, routers) within the Internet are completely oblivious to the connection. This is because a TCP connection consists of nothing more than allocated resources (buffers) and state variables in the end systems. The packet switches do not maintain any connection-state information.

Things to Remember:

Goal : data transfer between end systems

Handshaking: setup (prepare for) data transfer ahead of time

- Hello, hello back human protocol
- set up .state" in two communicating hosts

TCP -Transmission Control Protocol - Internet's connection oriented service

The Internet's connection-oriented service comes bundled with several other services, including reliable data transfer, flow control, and congestion control. By reliable data transfer, we mean that an application can rely on the connection to deliver all of its data without error and in the proper order.

Reliability in the Internet is achieved through the use of acknowledgements and retransmissions. To get a preliminary idea about how the Internet implements the reliable transport service, consider an application that has established a connection between end systems A and B:

- When end system B receives a packet from A, it sends an acknowledgement; when end system A receives the acknowledgement, it knows that the corresponding packet has definitely been received.
- When end system A doesn't receive an acknowledgement, it assumes that the packet it sent was not received by B; it therefore retransmits the packet.

Flow control makes sure that neither side of a connection overwhelms the other side by sending too many packets too fast. Indeed, the application at one side of the connection may not be able to process information as quickly as it receives the information. Therefore, there is a risk of overwhelming either side of an application. The flow-control service forces the sending end system to reduce its rate whenever there is such a risk. We shall see that the Internet implements the flow control service by using sender and receiver buffers in the communicating end systems. The Internet's congestion-control service helps prevent the Internet from entering a state of gridlock.

When a router becomes congested, its buffers can overflow and packet loss can occur. In such circumstances, if every pair of communicating end systems continues to pump packets into the network as fast as they can, gridlock sets in and few packets are delivered to their destinations. The Internet avoids this problem by forcing end systems to decrease the rate at which they send packets into the network during periods of congestion. End systems are alerted to the existence of severe congestion when they stop receiving acknowledgements for the packets they have sent.

We emphasize here that although the Internet's connection-oriented service comes bundled with reliable data transfer, flow control, and congestion control, these three features are by no means essential components of a connection-oriented service. A different type of computer network may provide a connection-oriented service to its applications without bundling in one or more of these features. Indeed, any protocol that performs handshaking between the communicating entities before transferring data is a connection-oriented service.

The Internet's connection-oriented service has a name -TCP (Transmission Control Protocol); the initial version of the TCP protocol is defined in the Internet Request for Comments RFC 793 [RFC 793]. The services that TCP provides to an application include reliable transport, flow control, and congestion control. It is important to note that an application need only care about the services that are provided; it need not worry about how TCP actually implements reliability, flow control, or congestion control.

Things to Remember:

TCP service [RfC 793]

Reliable, in-order byte-stream data transfer : acknowledgements and retransmissions

Flow control: sender won't overwhelm receiver

Congestion control: senders “slow down sending rate" when network congested

GOTO TOP

Connection Less Service

There is no handshaking with the Internet's connectionless service. When one side of an application wants to send packets to another side of an application, the sending application simply sends the packets. Since there is no handshaking procedure prior to the transmission of the packets, data can be delivered faster. But there are no acknowledgements either, so a source never knows for sure which packets arrive at the destination. Moreover, the service makes no provision for flow control or congestion control. The Internet's connectionless service is provided by User Datagram Protocol (UDP); UDP is defined in the Internet RFC 768.

Most of the more familiar Internet applications use TCP, the Internet's connection-oriented service. These applications include Telnet (remote login), SMTP (for electronic mail), FTP (for file transfer), and HTTP (for the Web). Nevertheless, UDP, the Internet's connectionless service, is used by many applications, including many of the emerging multimedia applications, such as Internet phone, audio-on-demand, and video conferencing.

Things to Remember:

UDP - User Datagram Protocol [RFC 768]:

Unreliable data transfer

No flow control

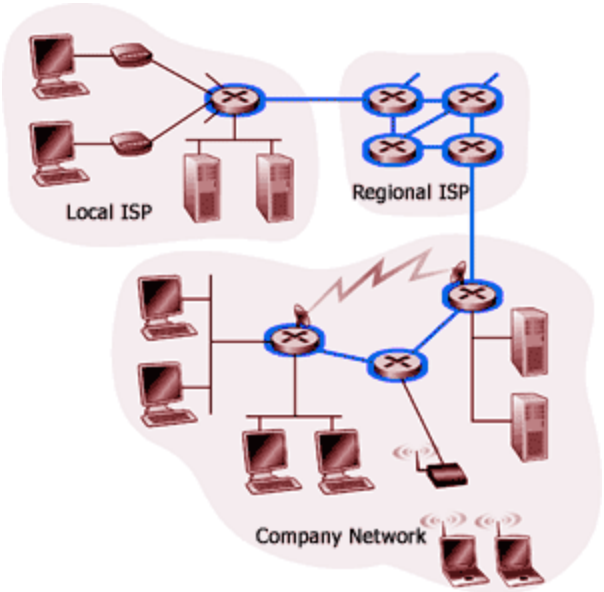
No congestion control

Applications using TCP: HTTP (WWW), FTP (File Transfer),Telnet (remote login), SMTP (email)

Applications using UDP: Streaming media, Teleconferencing,Internet telephony

GOTO TOP

The Network Core



There are two fundamental approaches towards building a network core: **circuit switching** and **packet switching**. In circuit-switched networks, the resources needed along a path (buffers, link bandwidth) to provide for communication between the end systems are reserved for the duration of the session. In packet-switched networks, these resources are not reserved; a session's messages use the resource on demand, and as a consequence, may have to wait (that is, queue) for access to a communication link

As a simple analogy, consider two restaurants -one that requires reservations and another that neither requires reservations nor accepts them. For the restaurant that requires reservations, we have to go through the hassle of first calling before we leave home. But when we arrive at the restaurant we can, in principle, immediately communicate with the waiter and order our meal. For the restaurant that does not require reservations, we don't need to bother to reserve a table. But when we arrive at the restaurant, we may have to wait for a table before we can communicate with the waiter.

Telephone networks are examples of circuit-switched networks. Consider what happens when one person wants to send information (voice or facsimile) to another over a telephone network. Before the sender can send the information, the network must first establish a connection between the sender and the receiver. In contrast with the TCP connection that we discussed in the previous section, this is a bona fide connection for which the switches on the path between the sender and receiver maintain connection state for that connection. In the jargon of telephony, this connection is called a circuit. When the network establishes the circuit, it also reserves a constant transmission rate in the network's links for the duration of the connection. This reservation allows the sender to transfer the data to the receiver at the guaranteed constant rate.

Things to Remember:

Network Core: Mesh of interconnected routers

The fundamental question: how is data transferred through net?

Circuit switching: Dedicated circuit per call: telephone net

Packet-switching: Data sent through net in discrete 'chunks'

Today's Internet is a quintessential packet-switched network. Consider what happens when one host wants to send a packet to another host over a packet-switched network. As with circuit switching, the packet is transmitted over a series of communication links. But with packet switching, the packet is sent into the network without reserving any bandwidth whatsoever. If one of the links is congested because other packets need to be transmitted over the link at the same time, then our packet will have to wait in a buffer at the sending side of the transmission line, and suffer a delay. The Internet makes its best effort to deliver the data in a timely manner, but it does not make any guarantees.

Not all telecommunication networks can be neatly classified as pure circuit-switched networks or pure packet-switched networks. For example, for networks based on the ATM technology, a connection can make a reservation and yet its messages may still wait for congested resources! Nevertheless, this fundamental classification into packet- switched and circuit-switched networks is an excellent starting point in understanding

telecommunication network technology.

GOTO TOP

Circuit Switching

This course is about computer networks, the Internet, and packet switching, not about telephone networks and circuit switching. Nevertheless, it is important to understand why the Internet and other computer networks use packet switching rather than the more traditional circuit-switching technology used in the telephone networks. For this reason, we now give a brief overview of circuit switching.

In this network, the three circuit switches are interconnected by two links; each of these links has n circuits, so that each link can support n simultaneous connections. The end systems (for example, PCs and workstations) are each directly connected to one of the switches. (Ordinary telephones are also connected to the switches, but they are not shown in the diagram.) Notice that some of the hosts have analogue access to the switches, whereas others have direct digital access.

For analogue access, a modem is required. When two hosts desire to communicate, the network establishes a dedicated end-to-end circuit between two hosts. (Conference calls between more than two devices are, of course, also possible. But to keep things simple, let us suppose for now that there are only two hosts for each connection.)

Thus, in order for host A to send messages to host B, the network must first reserve one circuit on each of the two links. Each link has n circuits; each end-to-end circuit over a link gets the fraction l/n of the link's bandwidth for the duration of the circuit.

Most types of telephone networks are examples of circuit-switched networks. Consider what happens when one person wants to send information (voice or facsimile) to another over a telephone network. Before the sender can send the information, the network must first establish a connection between the sender and the receiver.

Things to Remember:

End-end resources reserved for 'call'

Link bandwidth, switch capacity

Dedicated resources: no sharing

Circuit-like (guaranteed) performance

Call setup required

Things to Remember:

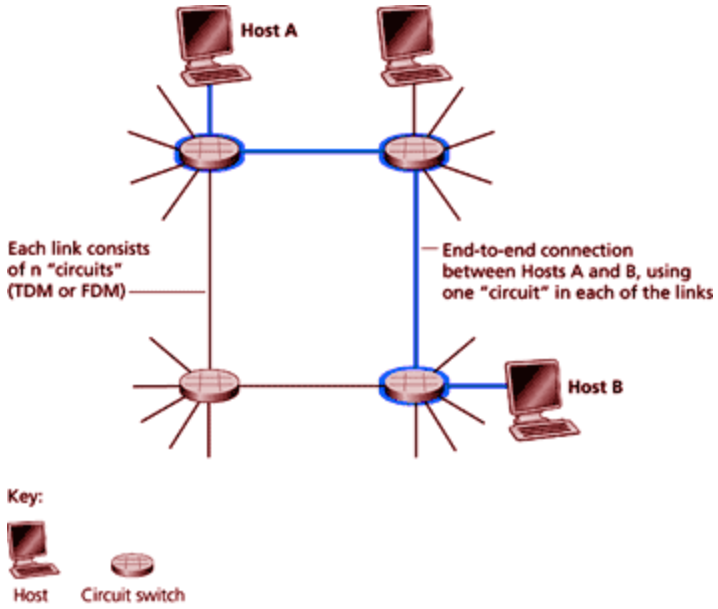
Network resources (e.g., bandwidth) divided into “pieces”

Pieces allocated to calls

Resource piece idle if not used by owning call (no sharing)

Dividing link bandwidth into “pieces”

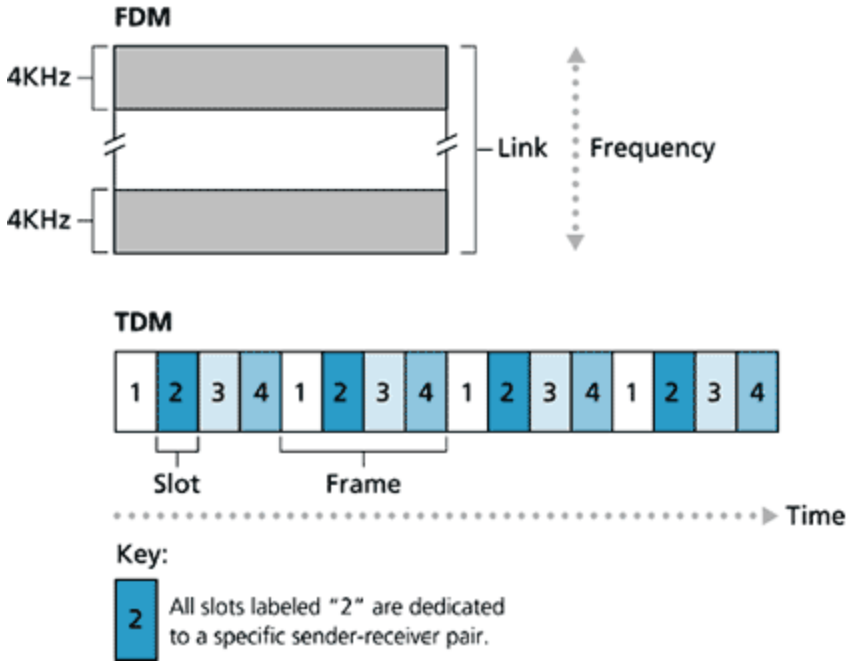
- Frequency division
- Time division



In contrast with the TCP connection that we discussed in the previous section, this is a bona fide connection for which the switches on the path between the sender and receiver maintain connection state for that connection. In the jargon of telephony, this connection is called a circuit. When the network establishes the circuit, it also reserves a constant transmission rate in the network's links for the duration of the connection. This reservation

allows the sender to transfer the data to the receiver at the guaranteed constant rate.

Circuit Switching: FDMA and TDMA



A circuit in a link is implemented with either frequency-division multiplexing (FDM) or time-division multiplexing (TDM). With FDM, the frequency spectrum of a link is shared among the connections established across the link. Specifically, the link dedicates a frequency band to each connection for the duration of the connection. In telephone networks, this frequency band typically has a width of 4 kHz (that is, 4,000 Hertz or 4,000 cycles per second). The width of the band is called, not surprisingly, the bandwidth. FM radio stations also use FDM to share the microwave frequency spectrum.

The trend in modem telephony is to replace FDM with TDM. Most links in most telephone systems in the United States and in other developed countries currently employ TDM. For a TDM link, time is divided into frames of fixed duration, and each frame is divided into a fixed number of time slots. When the network establishes a connection across a link, the network dedicates one time slot in every frame to the connection. These slots are dedicated for the sole use of that connection, with a time slot available for use (in every frame) to transmit the connection's data.

The previous diagram illustrates FDM and TDM for a specific network link. For FDM, the frequency domain is segmented into a number of circuits, each of bandwidth 4 KHz. For TDM, the time domain is segmented into four circuits; each circuit is assigned the same dedicated slot in the revolving TDM frames. The transmission rate of each circuit is equal to the frame rate multiplied by the number of bits in a slot. For example, if the link transmits 8,000 frames per second and each slot consists of8 bits, then the circuit transmission rate is 64 Kbps.

With FDM, each circuit continuously gets a fraction of the bandwidth. With TDM, each circuit gets all of the bandwidth periodically during brief intervals of time (that is, during slots).

Proponents of packet switching have always argued that circuit switching is wasteful because the dedicated circuits are idle during silent periods. For example, when one of the participants in a telephone call stops talking, the idle network resources (frequency bands or slots in the links along the connection's route) cannot be used by other ongoing connections. As another example of how these resources can be under utilized, consider a radiologist who uses a circuit-switched network to remotely access a series of x-rays. The radiologist sets up a connection, requests an image, contemplates the image, and then requests a new image. Network resources are wasted during the radiologist's contemplation periods. Proponents of packet switching also enjoy pointing out that establishing end-to-end circuits and reserving end-to-end bandwidth is complicated and requires complex signaling software to coordinate the operation of the switches along the end-to-end path.

Before we finish our discussion of circuit switching, let us work through a numerical example that should shed further insight on the matter. Let us consider how long it takes to send a file of 640 Kbits from host A to host B

over a circuit-switched network. Suppose that all links in the network use TDM with 24 slots and have a bit rate of 1.536 Mbps. Also suppose that it takes 500 msec to establish an end-to-end circuit before A can begin to transmit the file. How long does it take to send the file? Each circuit has a transmission rate of (1.536 Mbps)/24 = 64 Kbps, so it takes (640 Kbits)/(64 Kbps) = 10 seconds to transmit the file. To these 10 seconds we add the circuit establishment time, giving 10.5 seconds to send the file. Note that the transmission time is independent of the number of links. The transmission time would be 10 seconds if the end-to-end circuit passes through one link or one hundred links.

GOTO TOP

Packet Switching

We saw that application-level protocols exchange messages in accomplishing their task. Messages can contain anything the protocol designer desires. Messages may perform a control function (for example, the "Hi" messages in our handshaking example) or can contain data, such as an ASCII file, a Postscript file, a Web page, or a digital audio file. In modem packet-switched networks, the source breaks long messages into smaller packets. Between source and destination, each of these packets traverses communication links and packet switches (also known as routers).

Things to Remember:

Each end-to-end data stream divided into packets

- User A, B packets share network resources
- Each packet uses full link bandwidth
- Resources used as needed

Packets are transmitted over each communication link at a rate equal to the full transmission rate of the link. Most packet switches use store-and-forward transmission at the inputs to the links. Store-and- forward transmission means that the switch must receive the entire packet before it can begin to transmit the first bit of the packet onto the outbound link. Thus store-and-forward packet switches introduce a store-and-forward delay at the input to each link along the packet's route. This delay is proportional to the packet's length in bits. In particular, if a packet consists of L bits, and the packet is to be forwarded onto an outbound link of R bps, then the store-and-forward delay at the switch is L/R seconds.

Within each router there are multiple buffers (also called queues), with each link having an input buffer (to store packets that have just arrived to that link) and an output buffer. The output buffers playa key role in packet switching. If an arriving packet needs to be transmitted across a link but finds the link busy with the transmission of another packet, the arriving packet must wait in the output buffer. Thus, in addition to the store-and- forward delays, packets suffer output buffer queuing delays. These delays are variable and depend on the level of congestion in the network. Since the amount of buffer space is finite, an arriving packet may find that the buffer is completely filled with other packets waiting for transmission. In this case, packet loss will occur -either the arriving packet or one of the already-queued packets will be dropped. Returning to our restaurant analogy from earlier in this section, the queuing delay is analogous to the amount of time one spends waiting for a table. Packet loss is analogous to being told by the waiter that you must leave the premises because there are already too many other people waiting at the bar for a table.

Things to Remember:

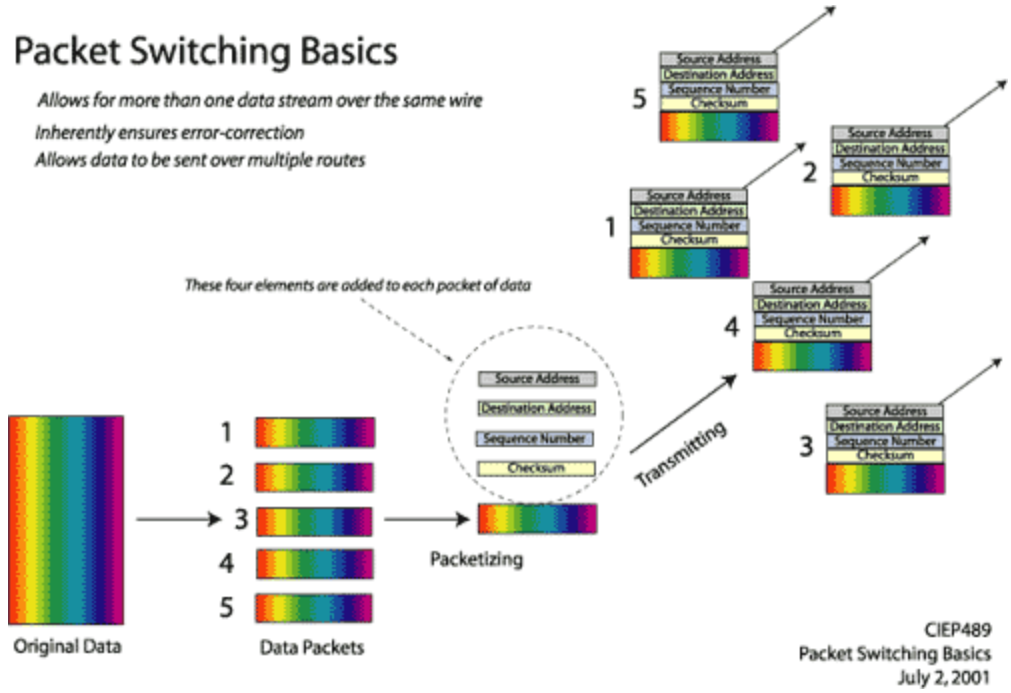
Resource contention:

Aggregate resource demand can exceed amount available

Congestion: packets queue, wait for link use

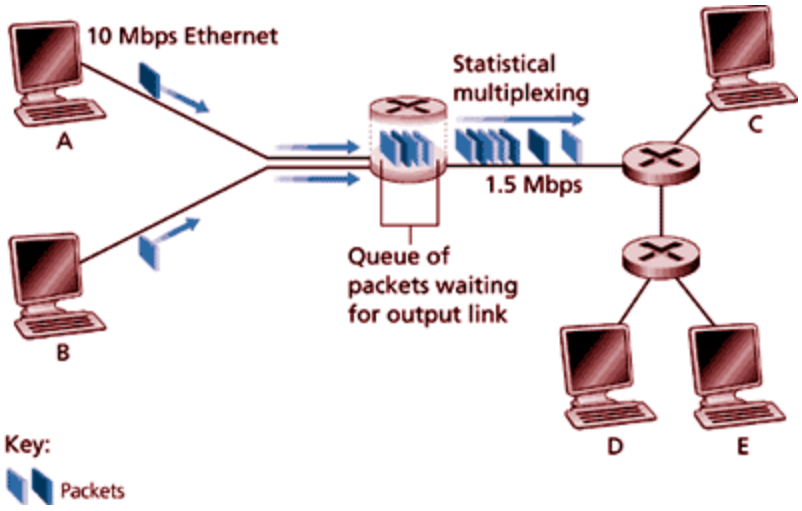
Store and forward: packets move one hop at a time

- transmit over link
- wait turn at next link



Note:

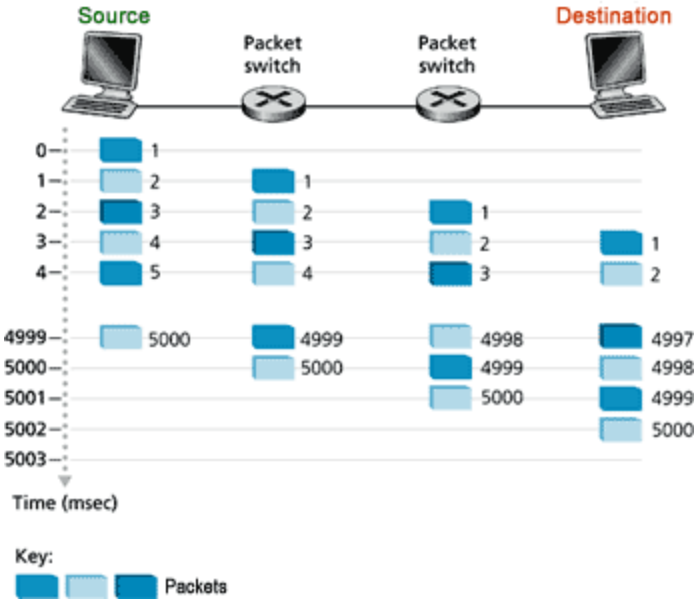
- **Bandwidth is not divided** into "pieces"
- There is **NO dedicated allocation** and
- **NO resource reservation**



Sequence of A & B packets does not have fixed pattern - **statistical multiplexing.**
In TDM each host gets same slot in revolving TDM frame.

This diagram illustrates a simple packet-switched network. Suppose Hosts A and Bare sending packets to Host E. Hosts A and B first send their packets along the 10 Mbps link to the first packet switch. The packet switch directs these packets to the 1.544 Mbps link. If there is congestion at this link, the packets queue in the link's output buffer before they can be transmitted onto the link. Consider now how Host A and Host B packets are transmitted onto this link. As shown in the above diagram, the sequence of A and B packets does not follow any periodic ordering; the ordering is random or statistical because packets are sent whenever they happen to be present at the link. For this reason, we often say that packet switching employs statistical multiplexing.

Statistical multiplexing sharply contrasts with time-division multiplexing (TDM), for which each host gets the same slot in a revolving TDM frame.



Packet Switching:

Store and Forward behaviour

- Break messages into smaller chunks called 'packets'
- store-and-forward: switch waits until chunk has completely arrived then forwards / routes

Application level protocol exchange messages in accomplishing the task. In modem packet switched networks the source breaks long messages in smaller packets. Most packet switches use store-and-forward transmission at the input to the links.

Store-and-forward transmission means that the switch must receive the entire packet before it can transmit the first bit of the packet on to the outbound link. Thus the store- and-forward packet switches induce a store-and-forward delay at the input link along the packet's route.

Message Segmentation - Java Applet

With this interactive applet, you will see the effect of pipelining when a large message is chopped up into many small packets. There are four nodes: a source, a destination and two intermediate store-and-forward switches. Each packet sent from the source must be transmitted over three links before it reaches the destination.

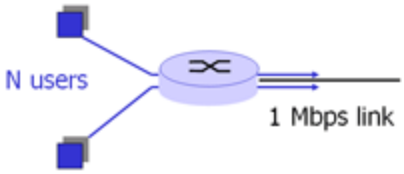
Message Segmentation - Click here to view applet

GOTO TOP

Packet Switching versus Circuit Switching

Packet switching allows more users to use network!

Having described circuit switching and packet switching, let us compare the two. Opponents of packet switching have often argued that packet switching is not suitable for real-time services (for example, telephone calls and video conference calls) because of its variable and unpredictable delays.



Proponents of packet switching argue that

1. it offers better sharing of bandwidth than circuit switching and
2. it is simpler, more efficient, and less costly to implement than circuit switching.

Generally speaking, people who do not like to hassle with restaurant reservations prefer packet switching to circuit switching.

Why is packet switching more efficient? Let us look at a simple example:

Suppose users share a **1 Mbps** link. Also suppose that each user alternates between periods of activity (when it generates data at a constant rate of 100 Kbps) and periods of inactivity (when it generates no data). Suppose further that a user is active only 10 percent of the time (and is idle drinking coffee during the remaining 90 percent of the time). With circuit switching, 100 Kbps must be reserved for each user at all times. Thus, the link can support only 10 simultaneous users. With packet switching, if there are 35 users, the probability that there are more than 10 simultaneously active users is approximately 0.0004.

If there are 10 or fewer simultaneously active users (which happens with probability 0.9996), the aggregate arrival rate of data is less than or equal to 1 Mbps (the output rate of the link). Thus, users' packets flow through the link essentially without delay, as is the case with circuit switching. When there are more than 10 simultaneously active users, then the aggregate arrival rate of packets will exceed the output capacity of the link.

Things to Remember:

1 Mbit link

Each user:

- 100 Kbps when "active"
- active 10% of tie

Circuit Switching: 10 users

Packet switching: with 35 users, probability >10 active less than 0.0004

Therefore the output queue will begin to grow (until the aggregate input rate falls back below 1 Mbps, at which point the queue will begin to diminish in length). Because the probability of having 10 or more simultaneously active users is extremely small, packet- switching almost always has the same delay performance as circuit switching, but does so while allowing for more than three times the number of users.

Although packet switching and circuit switching are both very prevalent in today's telecommunication networks, the trend is certainly in the direction of packet switching. Even many of today's circuit-switched telephone networks are slowly migrating towards packet switching. In particular, telephone networks often convert to packet switching for the expensive overseas portion of a telephone call.

Packet switching has yet another important advantage over message switching. As we will discuss later in this course, bit errors can be introduced into packets as they transit the network. When a switch detects an error in a packet, it typically discards the entire packet. So, if the entire message is a packet and one bit in the message gets corrupted, the entire message is discarded. If, on the other hand, the message is segmented into many packets and one bit in one of the packets is corrupted, then only that one packet is discarded.

Packet switching is not without its disadvantages, however.

We will see that each packet or message must carry, in addition to the data being sent from the sending application to the receiving application, an amount of control information. This information, which is carried in the packet or message header, might include the identity of the sender and receiver and a packet or message identifier (for example, number). Since the amount of header information would be approximately the same for a message or a packet, the amount of header overhead per byte of data is higher for packet switching than for message switching.

Things to Remember:

Is packet switching a 'slam dunk winner'?

Great for bursty data

Resource sharing
N o call setup

Excessive congestion: packet delay and loss

Protocols needed for reliable data transfer, congestion control

Discussion Question: How can circuit-like behaviour be provided considering bandwidth guarantees are needed for audio/video applications?

GOTO TOP

Packet Switched Networks : Routing

Goal: move packets among routers from source to destination

There are two broad classes of packet-switched networks: datagram networks and virtual circuit networks. They differ according to whether they route packets according to host destination addresses or according to virtual circuit numbers.

We shall call any network that routes packets according to host destination addresses a datagram network. The IP protocol of the Internet routes packets according to the destination addresses; hence the Internet is a

datagram network.

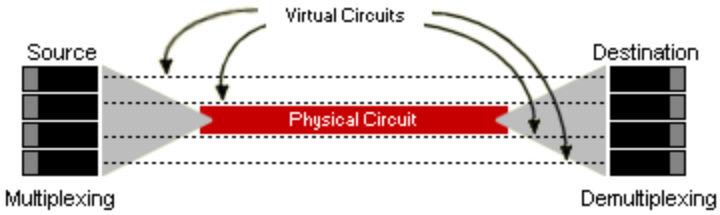
We shall call any network that routes packets according to virtual circuit numbers a virtual circuit network. Examples of packet-switching technologies that use virtual circuits include X.25, frame relay, and Asynchronous Transfer Mode (ATM).

GOTO TOP

Virtual Circuit Networks

A virtual circuit (V C) consists of

1. A path (that is, a series of links and packet switches) between the source and destination hosts
2. Virtual circuit numbers, one number for each link along the path, and
3. Entries in VC-number translation tables in each packet switch along the path.



Multiplexing Multiple Virtual Circuits

Things to Remember:

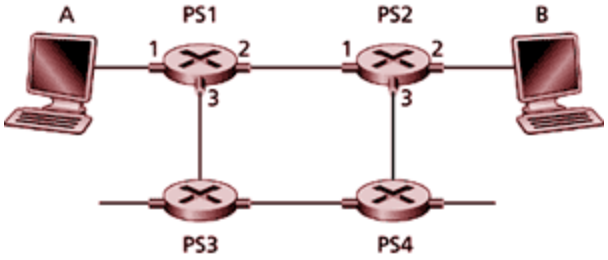
Virtual circuit network:

Each packet carries tag (virtual circuit ID). tag determines next hop

Fixed path determined at call setup time. remains fixed through call

Routers maintain per-call state

Once a VC is established between source and destination, packets can be sent with the appropriate VC numbers. Because a VC has a different VC number on each link, an intermediate packet switch must replace the VC number of each traversing packet with a new one. The new VC number is obtained from the VC-number translation table.



To illustrate the concept, consider the network shown in the figure. Suppose host A requests that the network establish a VC between itself and host B. Suppose that the network chooses the path A-PS1-PS2-B and assigns VC numbers 12, 22, 32 to the three links in this path. Then, when a packet as part of this VC leaves host A, the value in the VC-number field is 12; when it leaves PS1, the value is 22; and when it leaves PS2, the value is 32. The numbers next to the links of PS1 are the interface numbers.

GOTO TOP

Datagram Networks

Datagram networks are analogous in many respects to the postal services. When a sender sends a letter to a destination, the sender wraps the letter in an envelope and writes the destination address on the envelope. This destination address has a hierarchical structure. For example, letters sent to a location in the United Kingdom include the country (England), the county (for example, Lancashire), the city (for example, Manchester), the street (for example, Caroline Street) and the number of the house on the street (for example, 306). The postal services use the address on the envelope to route the letter to its destination. For example, if the letter is sent from United Arab Emirates, then a postal office in United Arab Emirates will first direct the

letter to a postal centre in the United Kingdom. This postal centre in the United Kingdom will then send the letter to a postal centre in Manchester. Finally, a mail person working in Manchester will deliver the letter to its ultimate destination.

In a datagram network, each packet that traverses the network contains in its header the address of the destination. As with postal addresses, this address has a hierarchical structure. When a packet arrives at a packet switch in the network, the packet switch examines a portion of the packet's destination address and forwards the packet to an adjacent switch. More specifically, each packet switch has a routing table that maps destination addresses (or portions of the destination addresses) to an outbound link. When a packet arrives at a switch, the switch examines the address and indexes its table with this address to find the appropriate outbound link. The switch then sends the packet into this outbound link.

Things to Remember:

Datagram network:

Destination address determines next hop

Routes may change during session

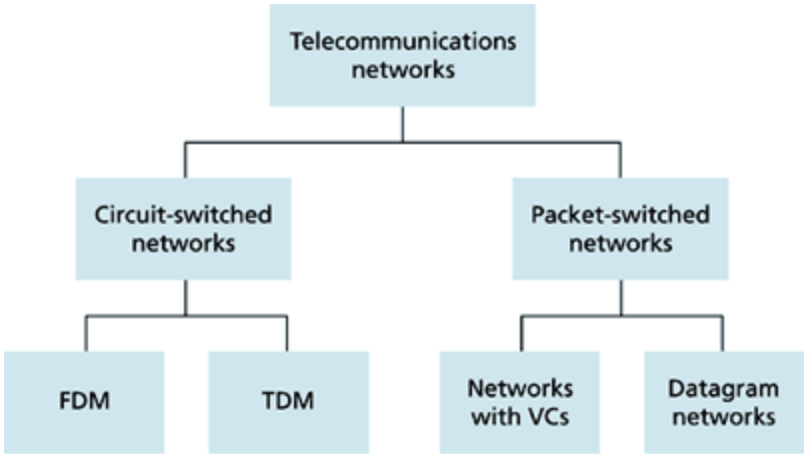
Analogy: driving, asking directions

The whole routing process is also analogous to the car driver who does not use maps but instead prefers to ask for directions.

For example, suppose Joe is driving from Philadelphia to 156 Lakeside Drive in Orlando, Florida. Joe first drives to his neighbourhood gas station and asks how to get to 156 Lakeside Drive in Orlando, Florida. The gas station attendant extracts the Florida portion of the address and tells Joe that he needs to get onto the interstate highway 1-95 South, which has an entrance just next to the gas station. He also tells Joe that once he enters Florida he should ask someone else there. Joe then takes 1-95 South until he gets to Jacksonville, Florida, at which point he asks another gas station attendant for directions. The attendant extracts the Orlando portion of the address and tells Joe that. he should continue on 1-95 to Daytona Beach and then ask someone else. In Daytona Beach another gas station attendant also extracts the Orlando portion of the address and tells Joe that he should take 1-4 directly to Orlando. Joe takes 1-4 and gets off at the Orlando exit. Joe goes to another gas station attendant, and this time the attendant extracts the Lakeside Drive portion of the address and tells Joe the road he must follow to get to Lakeside Drive. Once Joe reaches Lakeside Drive he asks a kid on a bicycle how to get to his destination. The kid extracts the 156 portion of the address and points to the house. Joe finally reaches his ultimate destination.

How would you like to actually see the route that packets take in the Internet? We now invite you to get your hands dirty by interacting with the Tracert program (Windows) or traceroute (Linux).

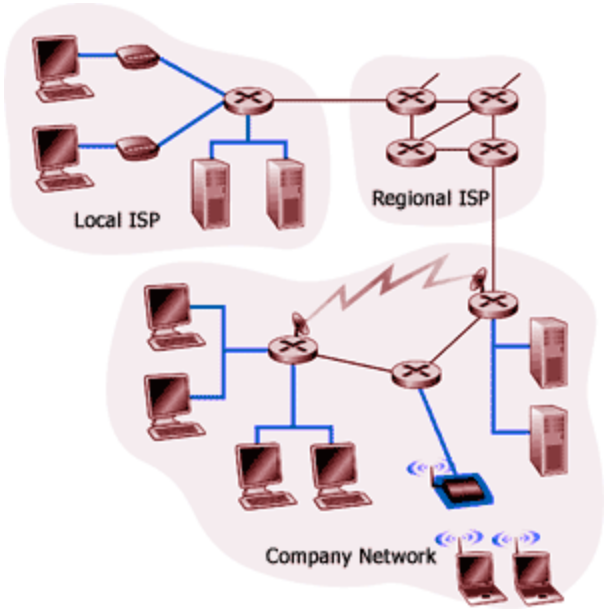
Network Taxonomy



- Datagram network is not either connection-oriented or connectionless.
- Internet provides both connection-oriented (TCP) and connectionless services (UDP) to apps.

GOTO TOP

Access Networks



We have examined the roles of end systems and routers in network architecture. In this section we consider the access network -the physical link(s) that connect an end system to its edge router -that is, to the first router on a path from the end system to any other distant end system. Since access network technology is closely tied to physical media technology (fibre, coaxial pair, twisted-pair telephone wire, radio spectrum), we consider these two topics together in this section.

Access networks can be loosely divided into three categories:

- Residential access networks - connecting a home end system into the network.
- Institutional access networks - connecting an end system in a business or educational institution into the network.
- Mobile access networks - connecting a mobile end system into the network.

These categories are not hard and fast; some corporate end systems may well use the access network technology that we ascribe to residential access networks, and vice versa. The following descriptions are meant to hold for the common (if not every) case.

Things to Remember:

How to connect end systems to edge router?

- Residential access nets
- Institutional access networks (school, company)
- Mobile access networks

Discussion Question: What are the different ways of connecting an end system to an edge router?

GOTO TOP

Residential Access Networks

A residential access network connects a home end system (typically a PC, but perhaps a Web TV or other residential system) to an edge router. Probably the most common form of home access is by use of a modem over a POTS (Plain Old Telephone System) dialup line to an Internet Service Provider (ISP). The home modem converts the digital output of the PC into analogue format for transmission over the analogue phone line. A modem in the ISP converts the analogue signal back into digital form for input to the ISP router. In this case, the access network is simply a point-to-point dialup link into an edge router. The point-to-point link is your ordinary twisted-pair phone line.

GOTO TOP

Point to Point Access

Today's modem speeds allow dialup access at rates up to 56 Kbps. However, due to the poor quality of twisted-pair line between many homes and ISPs, many users get an effective rate significantly less than 56 Kbps.

Whereas dialup modems require conversion of the end system's digital data into analogue form for transmission, so-called narrowband ISDN technology (Integrated Services Digital Network) allows for all-digital transmission of data from a home end system over ISDN 'telephone' lines to a phone company central office. Although ISDN was originally conceived as a way to carry digital data from one end of the phone system to another, it is also an important network access technology that provides higher speed access (for example, 128 Kbps) from the home into a data network such as the Internet. In this case, ISDN can simply be thought of as a 'better modem'.

Things to Remember:

Dialup via modem

Up to 56Kbps direct access to router (often less)

Can't surf and phone at same time.

Dialup modems and narrowband ISDN are already widely deployed technologies. Two new technologies, Asymmetric Digital Subscriber Line (ADSL) and Hybrid Fibre Coaxial cable (HFC) are currently being deployed.

ADSL is conceptually similar to dialup modems: It is a new modem technology again running over existing twisted-pair telephone lines, but it can transmit at rates of up to about 8 Mbps from the ISP router to a home end system. The data rate in the reverse direction, from the home end system to the central office router, is less than 1 Mbps. The asymmetry in the access speeds gives rise to the term asymmetric in ADSL. The asymmetry in the data rates reflects the belief that a home user is more likely to be a consumer of information (bringing data into the home) than a producer of information.

ADSL uses frequency division multiplexing, as described in the previous section. In particular, ADSL divides the communication link between the home and the ISP into three non-overlapping frequency bands.

Things to Remember:

ADSL: asymmetric digital subscriber line

Up to 1 Mbps upstream (today typically < 256 kbps)

Up to 8 Mbps downstream (today typically < 1 Mbps)

FDM: 50 kHz - 1 MHz for downstream

4 kHz - 50 kHz for upstream

0 kHz - 4 kHz for ordinary telephone

GOTO TOP

Cable Modems

One of the features of ADSL is that the service allows the user to make an ordinary telephone call, using the POTS channel, while simultaneously surfing the Web. This feature is not available with standard dialup modems. The actual amount of downstream and upstream bandwidth available to the user is a function of the distance between the home modem and the ISP modem, the gauge of the twisted-pair line, and the degree of electrical interference. For a high-quality line with negligible electrical interference, an 8 Mbps downstream transmission rate is possible if the distance between the home and the ISP is less than 3,000 meters; the downstream transmission rate drops to about 2 Mbps for a distance of6,000 meters. The upstream rate ranges from 16 Kbps to 1 Mbps.

ADSL, ISDN, and dialup modems all use ordinary phone lines, but HFC access networks are extensions of the current cable network used for broadcasting cable television. In a traditional cable system, a cable head end station broadcasts through a distribution of coaxial cable and amplifiers to residences, fibre optics (also to be discussed soon) connect the cable head end to neighbourhood-level junctions, from which traditional coaxial cable is then used to reach individual houses and apartments. Each neighbourhood juncture typically supports 500 to 5,000 homes.

Things to Remember:

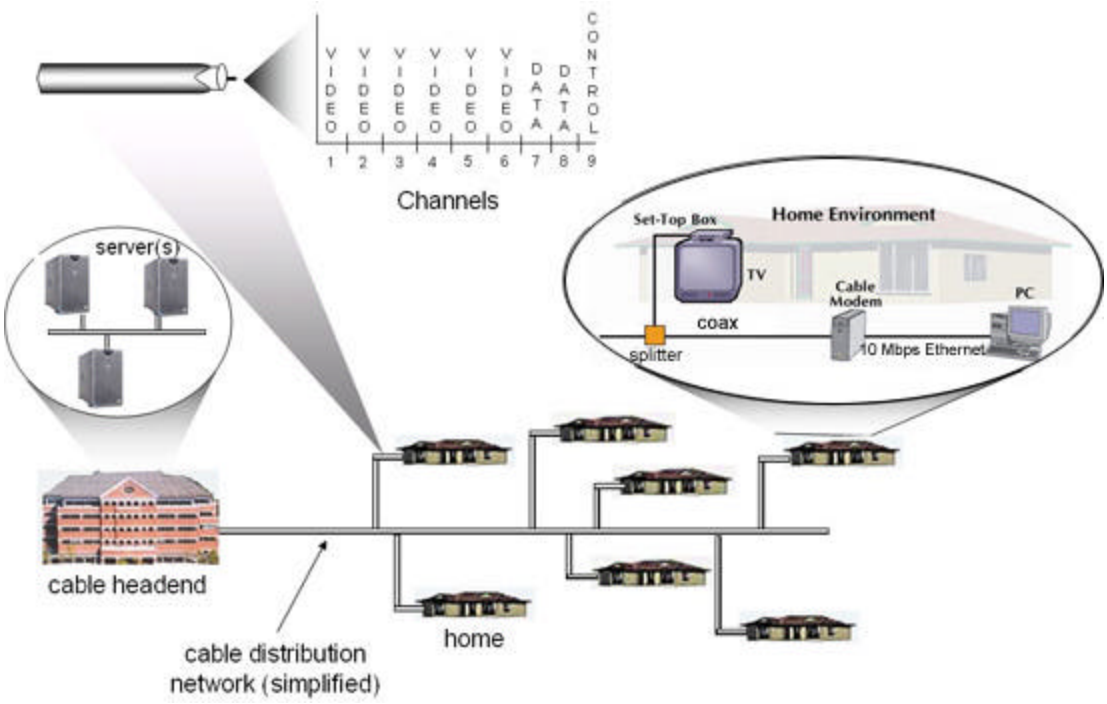
HFC: hybrid fiber coax

Asymmetric: up to 10Mbps upstream, 1 Mbps downstream

Network of cable and fiber attaches homes to ISP router

- Shared access to router among home
- Issues: congestion, dimensioning

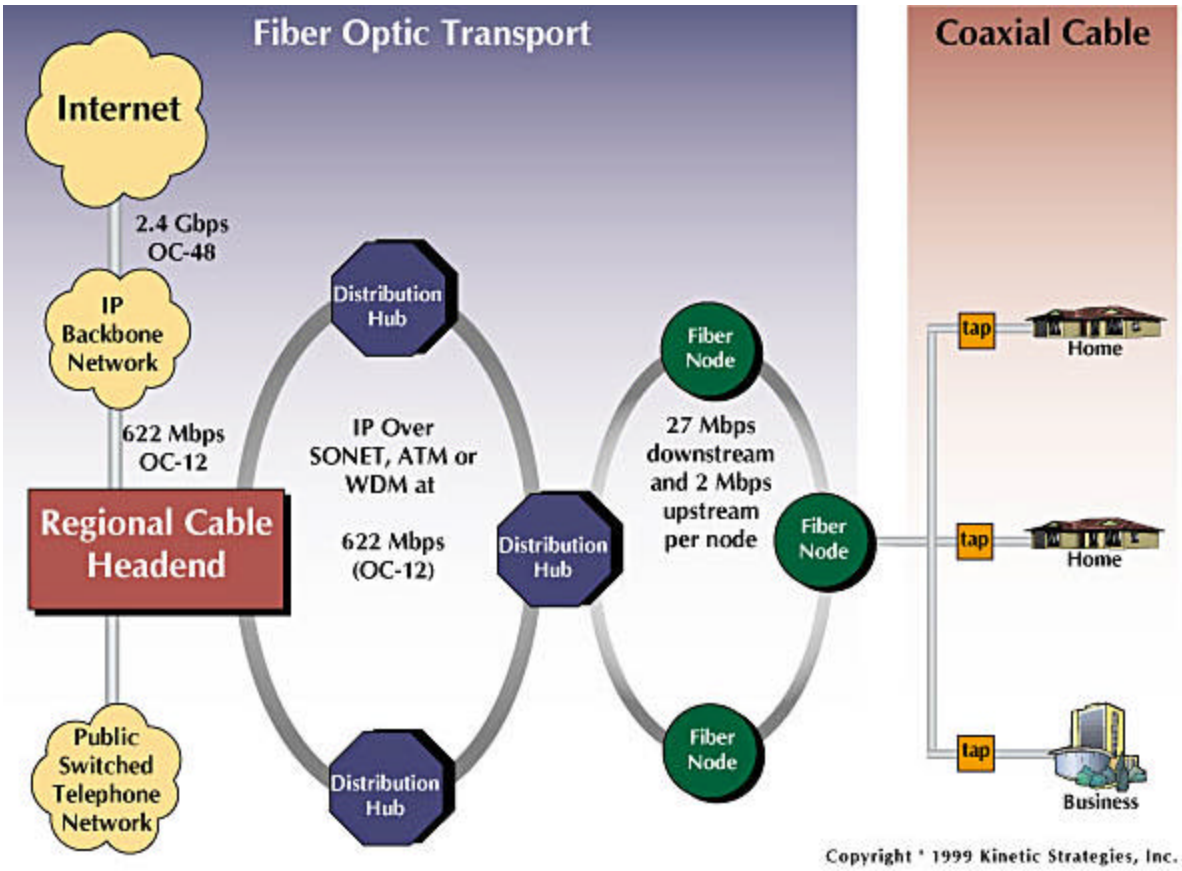
Deployment: available via cable companies, e.g., MediaOne



GOTO TOP

Cable Data Network Architecture

To offer high-speed Internet services, a cable operator creates a data network that operates over its hybrid fiber/coax (HFC) plant. The following diagram provides a high-level look at a typical large market cable network, including a regional cable headend (typically serving 200,000 to 400,000 homes), which feeds distribution hubs (each serving 20,000 to 40,000 homes) through a metropolitan fiber ring. At the distribution hub, signals are modulated onto analog carriers and then transported over fiber-optic lines to nodes serving 500 to 1,000 homes. From the node, these signals are carried via coaxial cable to a home or business.



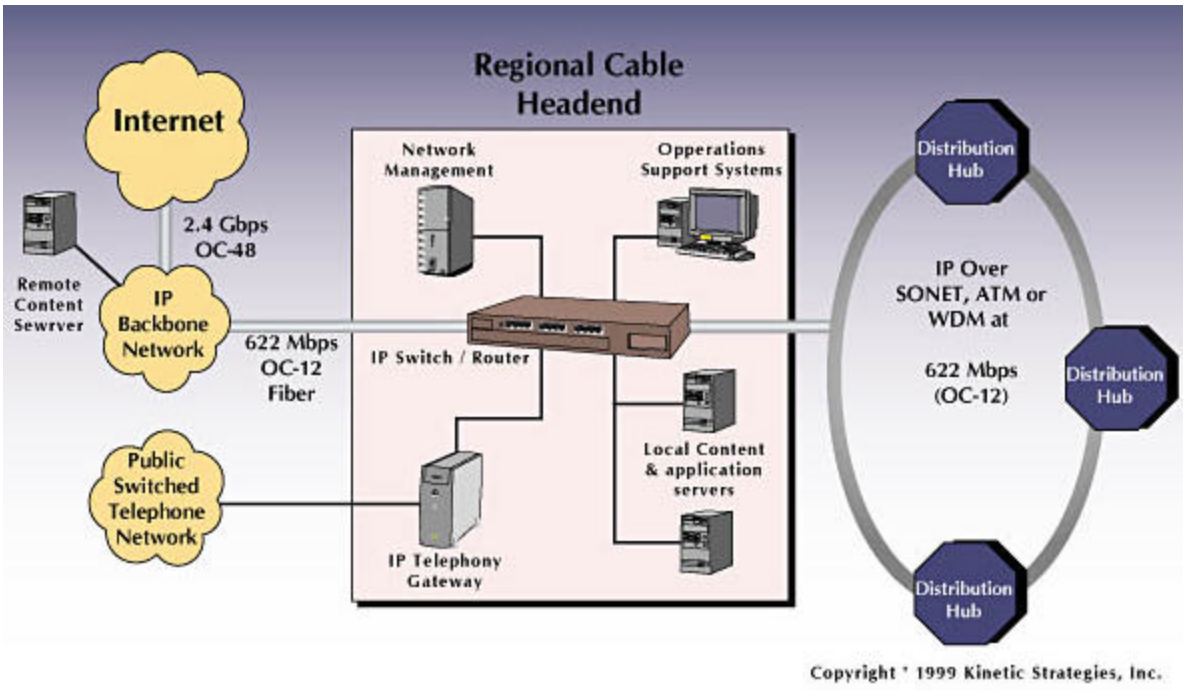
Source: http://www.cabledatacomnews.com/cmic/diagram.html

Regional Cable Headend

The regional cable headend serves as the local data network operations center. A carrier-class IP switch or router interfaces with a backbone data network, such as those operated by @Home or Road Runner, offering connectivity to remote content servers, as well as the global Internet.

This switch/router also connects to cable modem termination systems (CMTS) housed in the distribution hubs (hyperlink). Many cable operators are beginning to deploy high-capacity packet transport solutions over fiber rings connecting the CMTS units in their distribution hubs, such as Packet Over SONET (POS), at up to OC-12 speeds (622 Mbps).

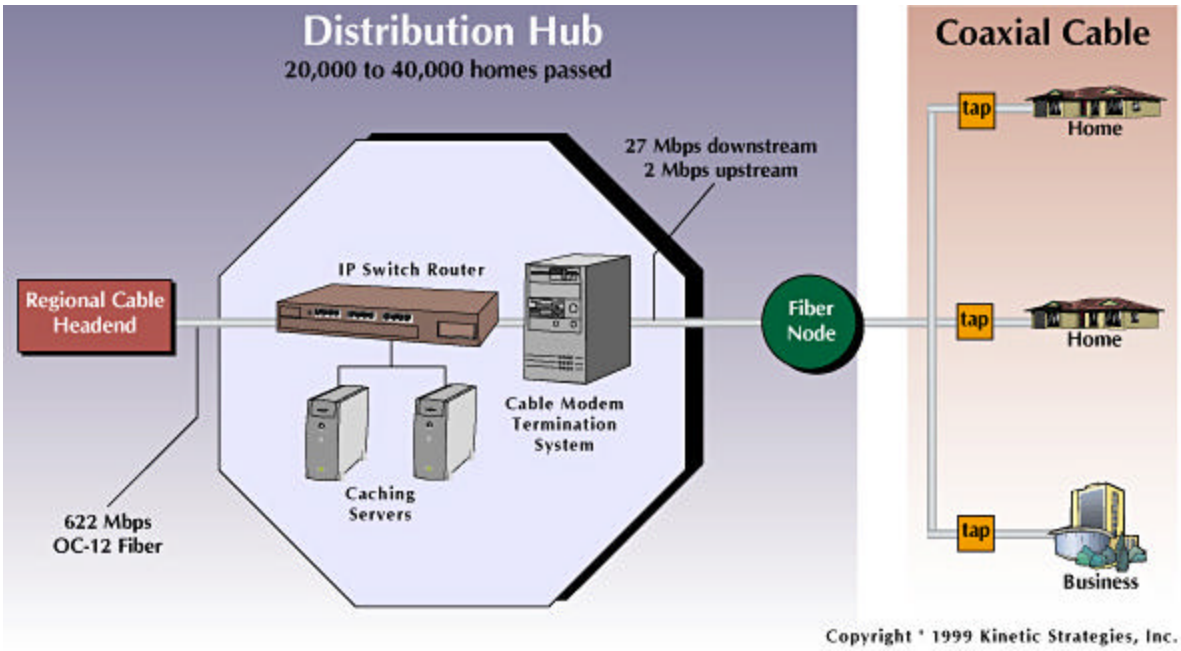
Content and application servers are typically at the regional cable headend, as are network management and operations support systems. If the cable operator were offering IP telephony, voice calls would be directed by the headend router to a IP telephony gateway, and then onto the public switched telephone network (PSTN).



Source: http://www.cabledatacomnews.com/cmic/headend.html

Distribution Hub

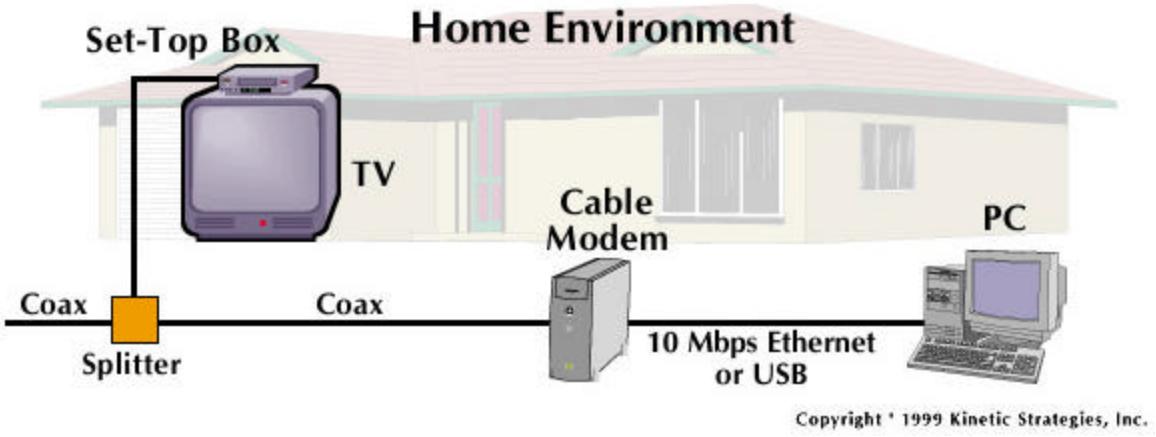
The hub is the interchange point between the regional fiber network and the cable plant. At the hub, the cable modem termination system (CMTS) coverts data from a wide area network (WAN) protocol, such as POS, into digital signals that are modulated for transmission over HFC plant, and then demodulated by the cable modem in the home or business. The CMTS unit provides a dedicated 27 Mbps downstream data channel that is shared by the 500 to 1,000 homes served by a fiber node, or group of nodes. Upstream bandiwdth per node typically ranges from 2 Mbps to 10 10 Mbps.



Source: http://www.cabledatacomnews.com/cmic/hub.html

Home Environment

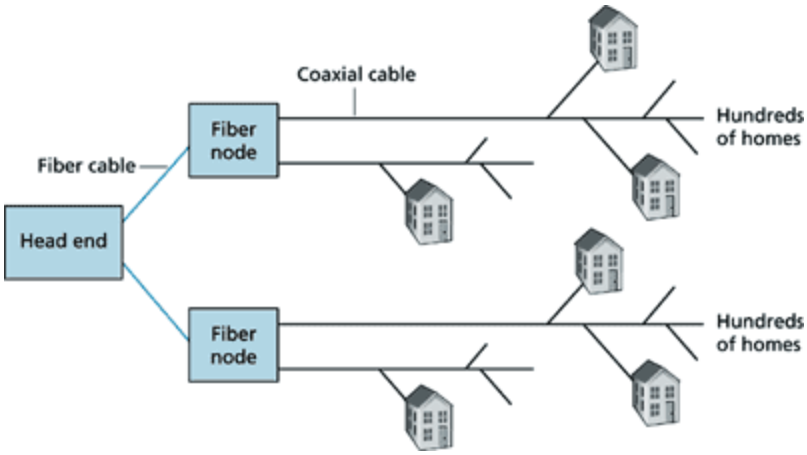
A splitter at the side of the home segments coaxial cable lines serving the cable modem and TV outlets. Cable modems currently connect to an Ethernet card in the PC with Category 5 cabling and RJ-45 connectors. Forthcoming cable modem products will also offer Universal Serial Bus (USB) connections



Source: http://www.cabledatacomnews.com/cmic/home.html

GOTO TOP

A Hybrid Fibre-Coax Access Network



As with ADSL, HFC requires special modems, called cable modems. Companies that provide cable Internet access require their customers to either purchase or lease a modem. One such company is Cyber Cable, which uses Motorola's Cyber Surfer Cable Modem and provides high-speed Internet access to most of the neighbourhoods in Paris. Typically, the cable modem is an external device and connects to the home PC through a 10-BaseT Ethernet port. Cable modems divide the HFC network into two channels, a downstream and an upstream channel. As with ADSL, the downstream channel is typically allocated more bandwidth and hence a larger transmission rate. For example, the downstream rate of the Cyber Cable system is 10 Mbps and the upstream rate is 768 Kbps. However, with HFC (and not with ADSL), these rates are shared among the homes, as we discuss next.

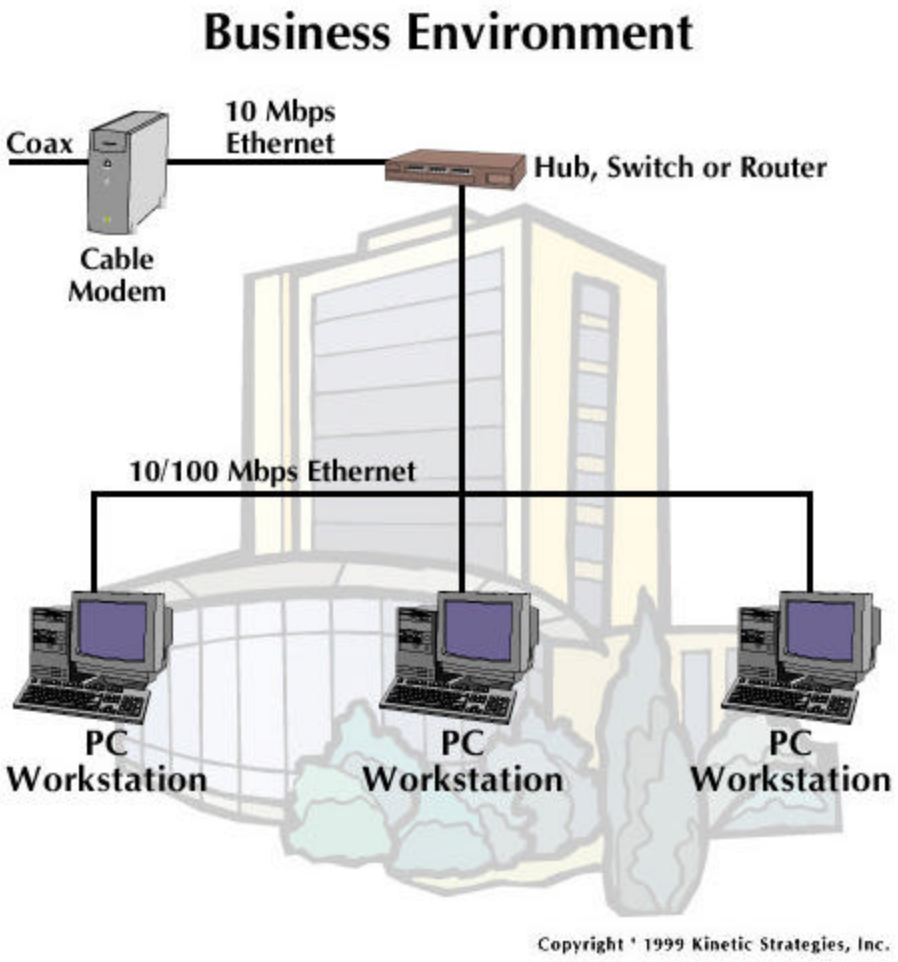
One important characteristic of HFC is that it is a shared broadcast medium. In particular, every packet sent by the head end travels downstream on every link to every home; and every packet sent by a home travels on the upstream channel to the head end. For this reason, if several users are receiving different Internet videos on the downstream channel, the actual rate at which each user receives its video will be significantly less than the downstream rate.

On the other hand, if all the active users are Web surfing, then each of the users may actually receive Web pages at the full downstream rate, as a small collection of users will rarely request a Web page at exactly the same time. Because the upstream channel is also shared, packets sent by two different homes at the same time will collide, which further decreases the effective upstream bandwidth.

Advocates of ADSL are quick to point out that ADSL is a point-to-point connection between the home and ISP, and therefore all the ADSL bandwidth is dedicated rather than shared. Cable advocates, however, argue that a reasonably dimensioned HFC network provides higher bandwidths than ADSL. The battle between ADSL and HFC for high speed residential access has clearly begun.

GOTO TOP

Company Access Networks



Source: http://www.cabledatacomnews.com/cmic/business.html

In company access networks, a local area network (LAN) is used to connect an end system to an edge router. As we will see in a later chapter, there are many different types of LAN technology. However, Ethernet technology is currently by far the most prevalent access technology in company networks.

Ethernet operates at 10 Mbps or 100 Mbps (and now even at 1 Gbps). It uses either twisted-pair copper wire or coaxial cable to connect a number of end systems with each other and with an edge router. The edge router is responsible for routing packets that have destinations outside of that LAN. Like HFC, Ethernet uses a shared medium, so that end users share the transmission rate of the LAN.

More recently, shared Ethernet technology has been migrating towards switched Ethernet technology. Switched Ethernet uses multiple coaxial cable or twisted-pair Ethernet segments connected at a 'switch' to allow the full bandwidth of an Ethernet to be delivered to different users on the same LAN simultaneously. We will explore shared and switched Ethernet in some detail in a later lesson.

Things to Remember:

Company / Univ local area network (LAN) connects end system to edge router

Ethernet:

- shared or dedicated link connects end system and router
- 10 Mbs, 100Mbps, Gigabit Ethernet

Deployment: institutions, home LANs happening now

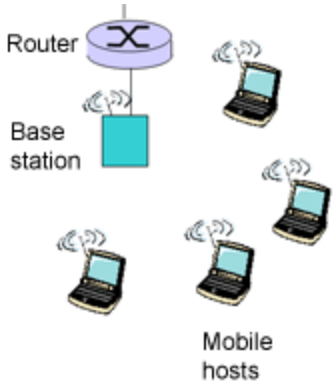
GOTO TOP

Mobile Access Networks

Mobile access networks use the radio spectrum to connect a mobile end system (for example, a laptop PC or a PDA with a wireless modem) to a base station. This base station, in turn, is connected to an edge router of a data network.

Wireless Access Networks

An emerging standard for wireless data networking is Cellular Digital Packet Data (CDPD). As the name suggests, a CDPD network operates as an overlay network (that is, as a separate, smaller virtual network, as a piece of the larger network) within the cellular telephone network. A CDPD network thus uses the same radio spectrum as the cellular phone system, and operates at speeds in the tens of Kbits per second. As with cable-based access networks and shared Ethernet, CDPD end systems must share the transmission media with other CDPD end systems within the cell covered by a base station.



A Media Access Control (MAC) protocol is used to arbitrate channel sharing among the CDPD end systems.

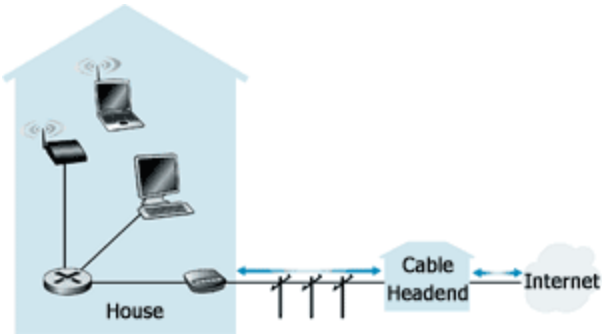
The CDPD system supports the IP protocol and thus allows an IP end system to exchange IP packets over the wireless channel with an IP base station. CDPD does not provide for any protocols above the network layer. From an Internet perspective, CDPD can be viewed as extending the Internet dial tone (that is, the ability to transfer IP packets) across a wireless link between a mobile end system and an Internet router.

Things to Remember:

Shared wireless access network connects end system to router via base station aka “access point”

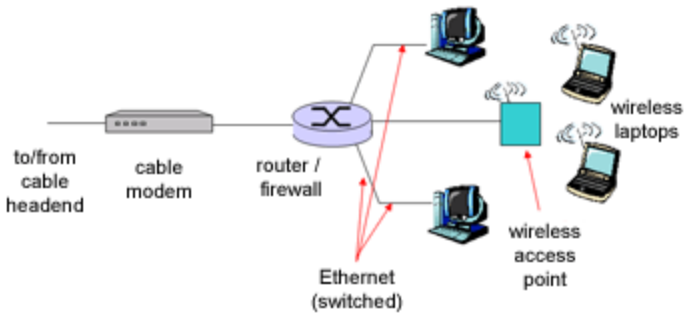
Wireless LANs: radio spectrum replaces wire

Home networks



Typical home network components:

- ADSL or cable modem
- router/firewall/NAT
- Ethernet
- wireless access point



GOTO TOP

Physical Media

In the previous subsection, we gave an overview of some of the most important access network technologies in the Internet. As we described these technologies, we also indicated the physical media used. For example, we said that HFC uses a combination of fibre cable and coaxial cable. We said that ordinary modems, ISDN, and ADSL use twisted-pair copper wire. And we

said that mobile access networks use the radio spectrum. In this subsection we provide a brief overview of these and other transmission media that are commonly employed in the Internet.

In order to define what is meant by a physical medium; let us reflect on the brief life of a bit. Consider a bit traveling from one end system, through a series of links and routers, to another end system. This poor bit gets transmitted many, many times! The source end system first transmits the bit, and shortly thereafter the first router in the series receives the bit; the first router then transmits the bit, and shortly afterwards the second router receives the bit, and so on.

Thus our bit, when traveling from source to destination, passes through a series of transmitter-receiver pairs. For each transmitter-receiver pair, the bit is sent by propagating electromagnetic waves or optical pulses across a physical medium. The physical medium can take many shapes and forms and does not have to be of the same type for each transmitter-receiver pair along the path.

Examples of physical media include twisted-pair copper wire, coaxial cable, multimode fibre-optic cable, terrestrial radio spectrum, and satellite radio spectrum.

Physical media fall into two categories: guided media and unguided media. With guided media, the waves are guided along a solid medium, such as a fibre-optic cable, a twisted-pair copper wire, or a coaxial cable. With unguided media, the waves propagate in the atmosphere and in outer space, such as in a digital satellite channel or in a CDPD system.

Things to Remember:

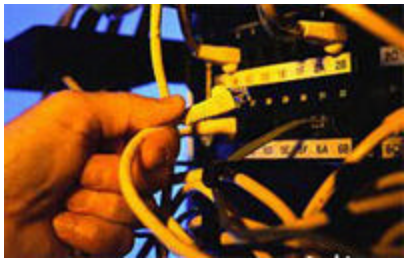
Physical Link: ransmitted data bit propagates across link

Guided Media: signals propagate in solid media: copper, fibre

Unguided Media: signals propagate freely. e.g., radio

GOTO TOP

Some Popular Physical Media



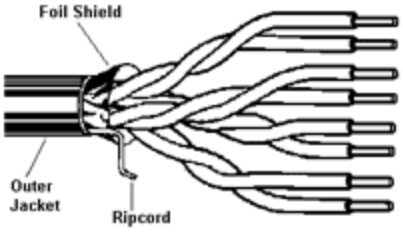
Suppose you want to wire a building to allow computers to access the Internet or an intranet. Should you use twisted-pair copper wire, coaxial cable, or fibre optics? Which of these media gives the highest bit rates over the longest distances? We shall address these questions below.

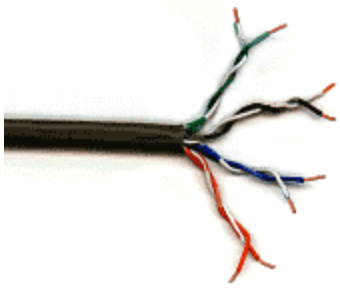
However, before we get into the characteristics of the various guided medium types, let us say a few words about their costs. The actual cost of the physical link (copper wire, fibre- optic cable, and so on) is often relatively minor compared with the other networking costs. In particular, the labour cost associated with the installation of the physical link can be orders of magnitude higher than the cost of the material.

For this reason, many builders install twisted pair, optical fibre, and coaxial cable to every room in a building. Even if only one medium is initially used, there is a good chance that another medium could be used in the near future, and so money is saved by not having to lay additional wires.

GOTO TOP

Twisted-Pair Copper Wire





The least-expensive and most commonly used transmission medium is twisted-pair copper wire. For over one-hundred years it has been used by telephone networks. In fact, more than 99 percent of the wired connections from the telephone handset to the local telephone switch use twisted-pair copper wire. Most of us have seen twisted-pair in our homes and work environments. Twisted-pair consists of two insulated copper wires, each about 1 mm thick, arranged in a regular spiral pattern. The wires are twisted together to reduce the electrical interference from similar pairs close by. Typically, a number of pairs are bundled together in a cable by wrapping the pairs in a protective shield. A wire pair constitutes a single communication link.

Twisted Pair

Unshielded Twisted Pair (UTP) is commonly used for computer networks within a building, that is, for local area networks (LANs). Data rates for LANs using twisted pair today range from 10 Mbps to 100 Mbps. The data rates that can be achieved depend on the thickness of the wire and the distance between transmitter and receiver.

Two types of UTP are common in LANs -category 3 and category 5:

- Category 3 corresponds to voice-grade twisted pair, commonly found in office buildings. Office buildings are often pre-wired with two or more parallel pairs of category 3 twisted pair; one pair is used for telephone communication, and the additional pairs can be used for additional telephone lines or for LAN networking. 10 Mbps Ethernet, one of the most prevalent LAN types, can use category 3 UTP.
- Category 5, with its more twists per centimetre and Teflon TM insulation, can handle higher bit rates. 100 Mbps Ethernet running on category 5 UTP has become very popular in recent years. In recent years, category 5 UTP has become common for pre-installation in new office buildings.

When fibre-optic technology emerged in the 1980s, many people disparaged twisted pair because of its relatively low bit rates. Some people even felt that fibre-optic technology would completely replace twisted pair. But twisted pair did not give up so easily. Modem twisted-pair technology, such as category 5 UTP, can achieve data rates of 100 Mbps for distances up to a few hundred meters. Even higher rates are possible over shorter distances. In the end, twisted pair has emerged as the dominant solution for high-speed LAN networking.

As discussed in the section on access networks, twisted pair is also commonly used for residential Internet access. We saw that dialup modem technology enables access at rates of up to 56 Kbps over twisted pair. We also saw that ISDN is available in many communities, providing access rates of about 128 Kbps over twisted pair. We also saw that ADSL (asymmetric digital subscriber loop) technology has enabled residential users to access the Internet at rates in excess of 6 Mbps over twisted pair.

Things to Remember:

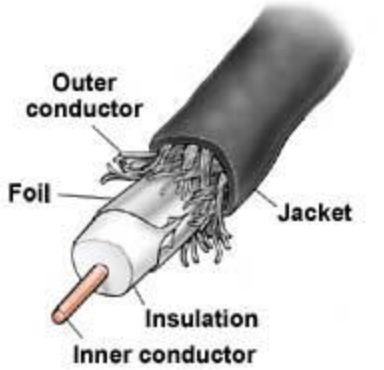
Twisted Pair (TP): two insulated copper wires

Category 3 TP: traditional phone wires, 10 Mbps Ethernet

Category 5 TP: 100Mbps Ethernet

GOTO TOP

Coaxial Cable



Like twisted pair, coaxial cable consists of two copper conductors, but the two conductors are concentric rather

than parallel. With this construction and a special insulation and shielding, coaxial cable can have higher bit rates than twisted pair. Coaxial cable comes in two varieties: baseband coaxial cable and broadband coaxial cable.

Baseband coaxial cable, also called 50-ohm cable, is about a centimetre thick, lightweight, and easy to bend. It is commonly used in LANs; in fact, the computer you use at work or at school is probably connected to a LAN with either baseband coaxial cable or with UTP.

Take a look at the connection to your computer's interface card:

- If you see a telephone-like jack and some wire that resembles telephone wire, you are using UTP .
- If you see a T-connector and a cable running out of both sides of the T - connector, you are using baseband coaxial cable.

The term baseband comes from the fact that the stream of bits is dumped directly into the cable, without shifting the signal to a different frequency band; 10 Mbps Ethemets can use either UTP or baseband coaxial cable.

GOTO TOP

Broadband Coaxial Cable

Broadband coaxial cable, also called 75 -ohm cable, is quite a bit thicker, heavier, and stiffer than the baseband variety. It was once commonly used in LAN s and can still be found in some older installations. For LANs, baseband cable is now preferable since it is less expensive, easier to physically handle, and does not require attachment cables.

Broadband cable, however, is quite common in cable television systems. As we saw earlier, cable television systems have recently been coupled with cable modems to provide residential users with Web access at rates of 10 Mbps or higher. With broadband coaxial cable, the transmitter shifts the digital signal to a specific frequency band, and the resulting analogue signal is sent from the transmitter to one or more receivers.

Both baseband and broadband coaxial cable can be used as a guided shared medium. Specifically, a number of end systems can be connected directly to the cable, and all the end systems receive whatever anyone of the computers transmits.

Things to Remember:

Coaxial cable:

Two concentric copper conductors

It is Bidirectional

Common use in 10 Mbps Ethernet

Baseband: single channel on cable, legacy Ethernet

Broadband: multiple channel on cable, HFC

GOTO TOP

Fibre Optics

An optical fibre is a thin, flexible medium that conducts pulses of light, with each pulse representing a bit. A single optical fibre can support tremendous bit rates, up to tens or even hundreds of gigabits per second. They are immune to electromagnetic interference, have very low signal attenuation up to 100 kilometres, and are very hard to tap. These characteristics have made fibre optics the preferred long-haul guided transmission media, particularly for overseas links.

Many of the long-distance telephone networks in the United States and elsewhere now use fibre optics exclusively. Fibre optics is also prevalent in the backbone of the Internet. However, the high cost of optical devices -such as transmitters, receivers, and switches - has hindered their deployment for short-haul transport, such as in a LAN or into the home in a residential access network.

Things to Remember:

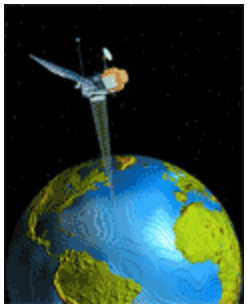
Fiber optic cable: glass fiber carrying light pulses, each pulse a bit

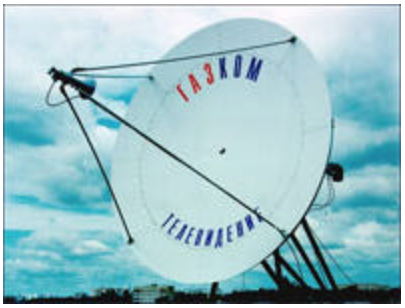
High-speed operation: 100 Mbps Ethernet, high-speed point-to-point transmission (e.g., 5 Gps)

Low error rate: repeaters spaced far apart ; immune to electromagnetic noise

GOTO TOP

Terrestrial and Satellite Radio Channels





Radio channels carry signals in the electromagnetic spectrum. They are an attractive media because they require no physical wire to be installed, can penetrate walls, provide connectivity to a mobile user, and can potentially carry a signal for long distances. The characteristics of a radio channel depend significantly on the propagation environment and the distance over which a signal is to be carried. Environmental considerations determine path loss and shadow fading (which decrease in signal strength as the signal travels over a distance, and around/through obstructing objects), multi path fading (due to signal reflection off interfering objects), and interference (due to other radio channels or electromagnetic signals).

Terrestrial radio channels can be broadly classified into two groups: those that operate as local area networks (typically spanning from ten to a few hundred meters) and wide-area radio channels that are used for mobile data services (typically operating within a metropolitan region). A number of wireless LAN products are on the market, operating in the range of one to tens of Mbps. Mobile data services typically provide channels that operate at tens of Kbps.

Things to Remember:

Radio: signal carried in electromagnetic spectrum

No physical “wire”

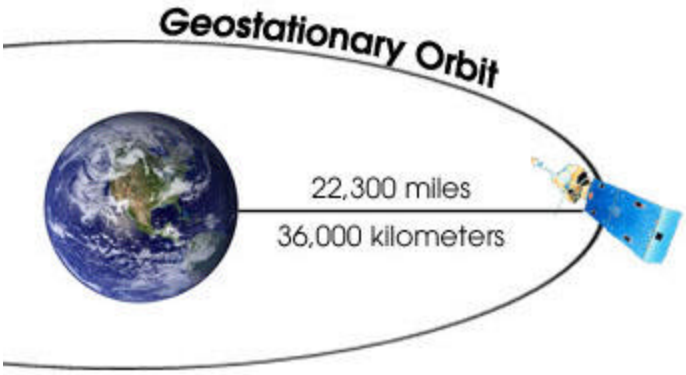
Bidirectional

Propagation environment effects:

- reflection
- obstruction by objects
- interference

A communication satellite links two or more Earth-based microwave transmitter/receivers, known as ground stations. The satellite receives transmissions on one frequency band, regenerates the signal using a repeater and transmits the signal on another frequency. Satellites can provide bandwidths in the gigabit per second range.

Two types of satellites are used in communications: geostationary satellites and low- altitude satellites.



- **Geostationary satellites** permanently remain above the same spot on Earth. This stationary presence is achieved by placing the satellite in orbit at 36,000 kilometres above Earth's surface. This huge distance from ground station through satellite back to ground station introduces a substantial signal propagation delay of 250 milliseconds. Nevertheless, satellite links, which can operate at speeds of hundreds of Mbps, are often

Things to Remember:

Radio link types:

Terrestrial Microwave
e.g. up to 45 Mbps channels

LAN (e.g., WaveLAN)
2Mbps, 11Mbps

Wide-area (e.g., cellular)
e.g. 3G: hundreds of kbps

Satellite

up to 50Mbps channel (or multiple smaller channels)

270 msec end-end delay

geosynchronous versus LEOS

used in telephone networks and in the backbone of the Internet.

- **Low-altitude satellites** are placed much closer to Earth and do not remain permanently above one spot on Earth. They rotate around Earth just as the Moon does. To provide continuous coverage to an area, many satellites need to be placed in orbit. There are currently many low-altitude communication systems in development. The Iridium system, for example, consists of 66 low-altitude satellites. Lloyd's Satellite Constellation Systems' Web page provides and collects information on Iridium as well as other satellite constellation systems. The low-altitude satellite technology may be used for Internet access sometime in the future.

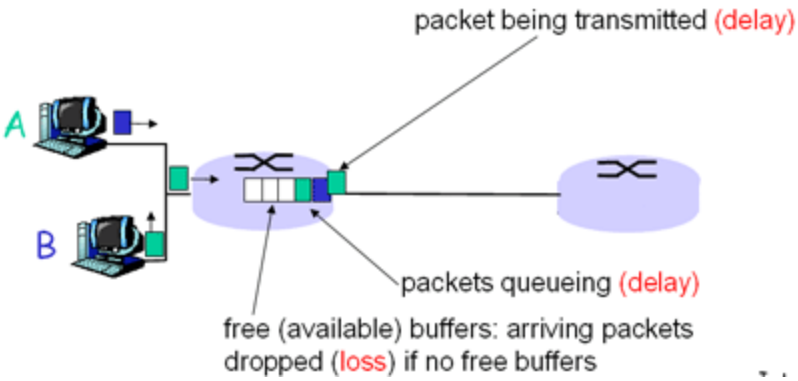
GOTO TOP

Delay and Loss in Packet-Switched Networks

Having briefly considered the major pieces of the Internet architecture -the applications, end systems, end-to-end transport protocols, routers, and links -let us now consider what can happen to a packet as it travels from its source to its destination.

Recall that a packet starts in a host (the source), passes through a series of routers, and ends its journey in another host (the destination). As a packet travels from one node (host or router) to the subsequent node (host or router) along this path, the packet suffers from several different types of delays at each node along the path. The most important of these delays are the nodal processing delay, queuing delay, transmission delay, and propagation delay. Together, these delays accumulate to give a total nodal delay.

In order to acquire a deep understanding of packet switching and computer networks, we must understand the nature and importance of these delays.



Things to Remember:

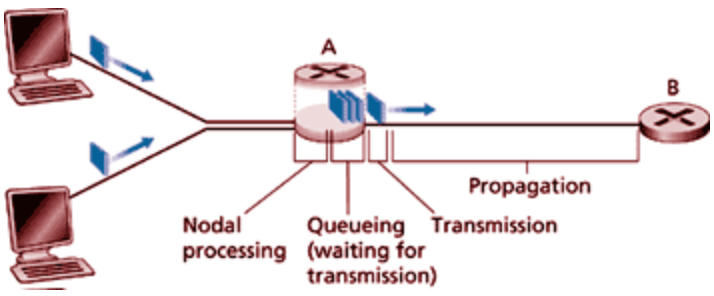
Packets queue in router buffers

Packet arrival rate to link exceeds output link capacity

Packets queue, wait for turn

GOTO TOP

Types of Delay



- **Processing delay** - the time required to examine the packet's header and determine where to direct the packet is part of the processing delay. The

processing delay can also include other factors, such as the time needed to check for bit-level errors in the packet that occurred in transmitting the packet's bits from the upstream router to router A. Processing delays in high-speed routers are typically on the order of microseconds Oi less. After this nodal processing, the router directs the packet to the queue that precedes the link to routei B.

Things to Remember:

1. Nodal processing:

check bit errors

determine output link

- **Queuing delay** - at the queue, the packet experiences a queuing delay as it waits to be transmitted onto the link. The queuing delay of a specific packet will depend on the number of other, earlier-arriving packets that are queued and waiting for transmission across the link. The delay of a given packet can vary significantly from packet to packet. If the queue is empty and no other packet is currently being transmitted, then our packet's queuing delay is zero. On the other hand, if the traffic is heavy and many other packets are also waiting to be transmitted, the queuing delay will be long. We will see shortly that the number of packets that an arriving packet might expect to find on arrival is a function of the intensity and nature of the traffic arriving to the queue. Queuing delays can be on the order of milliseconds to microseconds in practice.

Things to Remember:

2. Queueing

Time waiting at output link for transmission

Depends on congestion level of router

- **Transmission delay** - assuming that packets are transmitted in first-come-first-serve manner, as is common in the Internet, our packet can be transmitted once all the packets that have arrived before it have been transmitted. Denote the length of the packet by L bits, and denote the transmission rate of the link from router A to router B by R bits/sec. The rate R is determined by transmission rate of the link to router B. For example, for a 10-Mbps Ethernet link, the rate is R = 10 Mbps; for a 100-Mbps Ethernet link, the rate is R = 100 Mbps. The transmission delay is also known as the store-and-forward delay. This is the amount of time required to transmit all of the packet's bits into the link. Transmission delays are typically on the order of microseconds or less in practice.

Things to Remember:

3. Transmission delay:

R= link bandwidth (bps)

L= packet length (bits)

Time to send bits into link **= L/R**

- **Propagation delay** - once a bit is pushed onto the link, it needs to propagate to router B. The time required to propagate from the beginning of the link to router B is the propagation delay. The bit propagates at the propagation speed of the link. The propagation speed depends on the physical medium of the link (that is, multimode fibre, twisted-pair copper wire, and so on) and is in the range of:

  2 * 108 metres/see to 3 * 108 metres/sec

  which is equal to, or a little less than, the speed of light. The propagation delay is the distance between two routers divided by the propagation speed. That is, the propagation delay is d/s, where d is the distance between router A and router B and s is the propagation speed of the link. Once the last bit of the packet propagates to node B, it and all the preceding bits of the packet are stored in router B. The whole process then continues with router B now performing the forwarding. In wide-area networks, propagation delays are on the order of milliseconds.

Things to Remember:

4. Propagation delay:

d = length of physical link

s = propagation speed in medium (~2x108 m/sec)

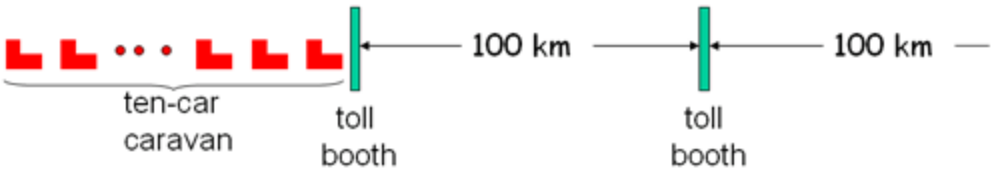
Propagation Delay = **d/s**

GOTO TOP

Comparing Transmission and Propagation Delay

Newcomers to the field of computer networking sometimes have difficulty understanding the difference between transmission delay and propagation delay. The difference is subtle but important. The transmission delay is the amount of time required for the router to push out the packet; it is a function of the packet's length and the transmission rate of the link, but has nothing to do with the distance between the routers. The propagation delay, on the other hand, is the time it takes a bit to propagate from one router to the next; it is a function of the distance between the two routers, but has nothing to do with the packet's length or the transmission rate of the link.

Caravan Analogy



- Cars “propagate” at 100 km/hr
- Toll booth takes 12 sec to service a car (transmission time)
- car~bit; caravan ~ packet
- Time to “push” entire caravan through toll booth onto highway = 12*10 = 120 sec
- Time for last car to propagate from 1st to 2nd toll both: 100km/(100km/hr)= 1 hr

Q: How long until caravan is lined up before 2nd toll booth?

A: 62 minutes

Transmission vs Propogation Delay - Java Applet

This simple applet illustrates one of the most fundamental concepts in computer networking: transmission delay versus propagation delay. Although this concept is discussed in detail in Lesson 1, an "interactive animation speaks a thousand words". You set the length of the link, the packet size, and the transmission speed; the applet shows the packet being sent from sender to receiver.

Transmission versus Propagation Delay - Click here to view applet

GOTO TOP

Queuing Delay

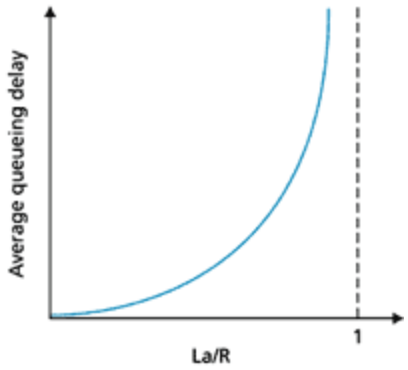
- R = Link bandwidth (bps)
- L = packet lenght (bits)
- a = average packet arrival rate

Traffic Intensit = La/R

La/R ~ 0: average queuing delay small

La/R =1: delays bcome large

La/R >1: more 'work' arriving than can be serviced, average delay is infinite!!



Queuing and Packet Loss - Java Applet

The most complicated and interesting component of end-to-end delay is queuing delay. In this applet, you specify the packet arrival rate and the link transmission speed. You'll then see packets arrive and queue for service. When the queue becomes full, you'll see the queue overflow– that is, packet loss. Enjoy!

Queueing Delay - Click here to view applet

GOTO TOP

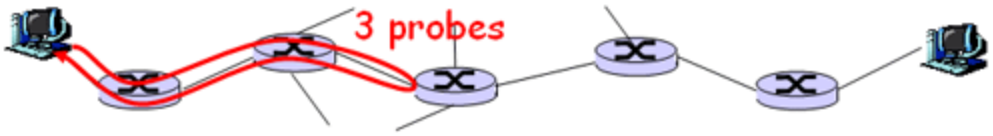
Real Internet Delays and Routes

What do “real” Internet delay & loss look like?

Traceroute program: provides delay measurement from source to router along end-end Internet path towards

destination. For all i:

- sends three packets that will reach router i on path towards destination
- router i will return packets to sender
- sender times interval between transmission and reply.



Example:

traceroute: gaia.cs.umass.edu to www.eurecom.fr

Three delay measements from gaia.cs.umass.edu to cs-gw.cs.umass.edu

```
1  cs-gw (128.119.240.254)  1 ms  1 ms  2 ms
2  border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145)  1 ms  1 ms  2 ms
3  cht-vbns.gw.umass.edu (128.119.3.130)  6 ms 5 ms 5 ms
4  jn1-at1-0-0-19.wor.vbns.net (204.147.132.129)  16 ms 11 ms 13 ms
5  jn1-so7-0-0-0.wae.vbns.net (204.147.136.136)  21 ms 18 ms 18 ms
6  abilene-vbns.abilene.ucaid.edu (198.32.11.9)  22 ms  18 ms  22 ms
7  nycm-wash.abilene.ucaid.edu (198.32.8.46)  22 ms  22 ms  22 ms
8  62.40.103.253 (62.40.103.253)  104 ms 109 ms 106 ms
9  de2-1.de1.de.geant.net (62.40.96.129)  109 ms 102 ms 104 ms
10  de.fr1.fr.geant.net (62.40.96.50)  113 ms 121 ms 114 ms
11  renater-gw.fr1.fr.geant.net (62.40.103.54)  112 ms  114 ms  112 ms
12  nio-n2.cssi.renater.fr (193.51.206.13)  111 ms  114 ms  116 ms
13  nice.cssi.renater.fr (195.220.98.102)  123 ms  125 ms  124 ms
14  r3t2-nice.cssi.renater.fr (195.220.98.110)  126 ms  126 ms  124 ms
15  eurecom-valbonne.r3t2.ft.net (193.48.50.54)  135 ms  128 ms  133 ms
16  194.214.211.25 (194.214.211.25)  126 ms  128 ms  126 ms
17  * * *
18  * * *
19  fantasia.eurecom.fr (193.55.113.142)  132 ms  128 ms  136 ms
```

* means no reponse (probe lost, router not replying)

Packet Loss

- Queue (aka buffer) preceding link in buffer has finite capacity
- When packet arrives to full queue, packet is dropped (aka lost)
- Lost packet may be retransmitted by previous node, by source end system, or not retransmitted at all

Exercise: Try a traceroute command if you are using Linux or tracert if you are using windows and note the result

Syntax: tracert <domainname>

Example: tracert nccedu.com

GOTO TOP

Protocol Layers and their Service Models

From our discussion so far, it is apparent that the Internet is an extremely complicated system. We have seen that there are many pieces to the Internet: numerous applications and protocols, various types of end systems and connections between end systems, routers, and various types of link-level media. Given this enormous complexity, is there any hope of organizing network architecture, or at least our discussion of network architecture? Fortunately, the answer to both questions is yes.

To reduce design complexity, network designers organize

Layer 1	Physical	1-PDU

protocols -and the network hardware and software that
implement the protocols -in layers. With a layered protocol architecture, each protocol belongs to one of the layers. It is important to realize that a protocol in layer n is distributed among the network entities (including end systems and packet switches) that implement that protocol, just as the functions in our layered airline architecture were distributed between the departing and arriving airports. In other words, there's a piece of layer n in each of the network entities. These pieces communicate with each other by exchanging layer-n messages. These messages are called layer-n protocol data units, or more commonly n-PDUs. The contents and format of an n-PDU, as well as the manner in which the n-PDUs are exchanged among the network elements, are defined by a layer-n protocol. When taken together, the protocols of the various layers are called the protocol stack.

Interestingly enough, this notion of relying on lower-layer services is prevalent in many other forms of communication. For example, consider ordinary postal mail. When you write a letter, you include envelope information such as the destination address and the return address with the letter. The letter, along with the address information, can be considered a PDU at the highest layer of the protocol stack. You then drop the PDU in a mailbox. At this point, the letter is out of your hands. The postal service may then add some of its own internal information onto your letter, essentially adding a header to your letter. For example, in the United States a barcode is often printed on your letter.

Once you drop your envelope into a mailbox, you rely on the postal service to deliver the letter to the correct destination in a timely manner. For example, you don't worry about whether a postal truck will break down while carrying the letter. Instead the postal service takes care of this, presumably with well-defined plans to recover from such failures. Furthermore, within the postal service itself there are layers, and the protocols at one layer rely on and use the services of the layer below.

Things to Remember:

Networks are complex!

Many “pieces”:

- Hosts
- Routers
- Links of various media
- Applications
- Protocols
- Hardware, software

In order for one layer to interoperate with the layer below it, the interfaces between the two layers must be precisely defined. Standards bodies define precisely the interlaces between adjacent layers (for example, the format of the PDUs passed between the layers) and permit the developers of networking software and hardware to implement the interior of the layers as they please. Therefore, if a new and improved implementation of a layer is released, the new implementation can replace the old implementation and, in theory, the layers will continue to interoperate.

Discussion Question: Is there any hope of organizing structure of network? Or at least our discussion of networks?

GOTO TOP

Layer Functions

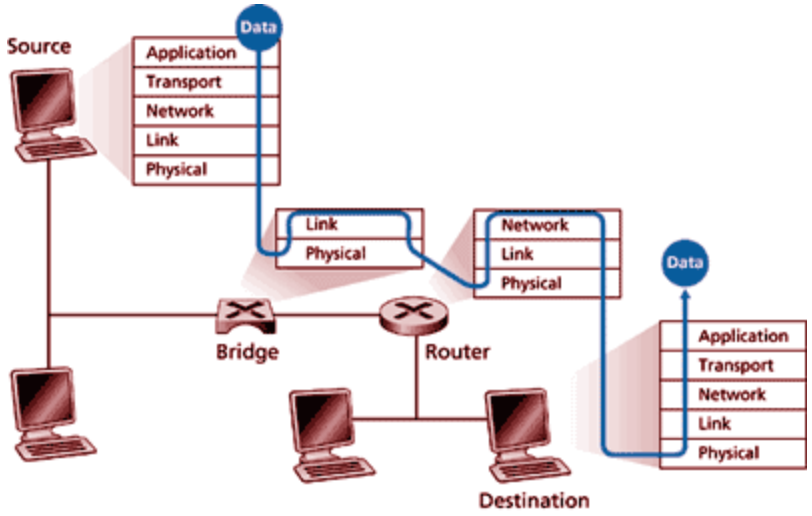
In a computer network, each layer may perform one or more of the following generic set of tasks:

- Error control, which makes the logical channel between the layers in two peer network elements more reliable.
- Flow control, which avoids overwhelming a slower peer with PDUs.
- Segmentation and reassembly, which at the transmitting side divides large data chunks into smaller pieces and at the receiving side reassembles the smaller pieces into the original large chunk.
- Multiplexing, which allows several higher-level sessions to share a single lower-level connection.

GOTO TOP

The Internet Protocol Stack, and Protocol Data Units

A protocol layer can be implemented in software, in hardware, or using a combination of the two. Application-layer protocols -such as HTTP and SMTP -are almost always implemented in software in the end systems; so are transport-layer protocols. Because the physical layer and data link layers are responsible for handling communication over a specific link, they are typically implemented in a network interface card (for example, Ethernet or ATM interlace cards) associated with a given link. The network layer is often a mixed implementation of hardware and software. We now summarize the Internet layers and the services they provide:



GOTO TOP

Application Layer

The application layer is responsible for supporting network applications. The application layer includes many protocols, including HTTP to support the Web, SMTP to support electronic mail, and FTP to support file transfer. We shall see in Lesson 2 that it is very easy to create our own new application-layer protocols.

GOTO TOP

Transport Layer

The transport layer provides the service of transporting application-layer messages between the client and server sides of an application. In the Internet there are two transport protocols, TCP and UDP, either of which can transport application-layer messages. TCP provides a connection-oriented service to its applications. This service includes guaranteed delivery of application-layer messages to the destination and flow control (that is, sender/receiver speed matching). TCP also segments long messages into shorter segments and provides a congestion control mechanism, so that a source throttles its transmission rate when the network is congested. The UDP protocol provides its applications a connectionless service, which (as we saw in the earlier section) is very much a no-frills service.

GOTO TOP

Network Layer

The network layer is responsible for routing datagrams from one host to another. The Internet's network layer has two principle components. It has a protocol that defines the fields in the IP datagram as well as how the end systems and routers act on these fields. This protocol is the celebrated IP protocol. There is only one IP protocol, and all Internet components that have a network layer must run the IP protocol. The Internet's network layer also contains routing protocols that determine the routes that datagrams take between sources and destinations. The Internet has many routing protocols. As we saw in the earlier sections, the Internet is a network of networks, and within a network, the network administrator can run any routing protocol desired. Although the network layer contains both the IP protocol and numerous routing protocols, it is often simply referred to as the IP layer, reflecting the fact that IP is the glue that binds the Internet together.

The Internet transport layer protocols (TCP and UDP) in a source host passes a transport- layer segment and a destination address to the IP layer, just as you give the postal service a letter with a destination address. The IP layer then provides the service of routing the segment to its destination. When the packet arrives at the destination, IP passes the segment to the transport layer within the destination.

GOTO TOP

Link Layer

The network layer routes a packet through a series of packet switches (called routers, in the Internet) between the source and destination. To move a packet from one node (host or packet switch) to the next node in the route, the network layer must rely on the services of the link layer. In particular, at each node IP passes the datagram to the link layer, which delivers the datagram to the next node along the route. At this next node, the link layer passes the IP datagram to the network layer. The process is analogous to the postal worker at a mailing centre who puts a letter into a plane that will deliver the letter to the next postal centre along the route. The services provided at the link layer depend on the specific link-layer protocol that is employed over the link. For example, some protocols provide reliable delivery on a link basis, that is, from transmitting node, over one link, to receiving node. Note that this reliable delivery service is different from the reliable delivery service of TCP, which provides reliable delivery from one end system to another. Examples of link layers include Ethernet and Point-to-Point Protocol (PPP); in some contexts, ATM and frame relay can be considered link layers. As datagrams typically need to traverse several links to travel from source to destination, a datagram may be handled by different link-layer protocols at different links along its route. For example, a datagram may be handled by Ethernet on one link and then PPP on the next link. IP will receive a different service from each of the different link-layer protocols.

GOTO TOP

Physical Layer

While the job of the link layer is to move entire frames from one network element to an adjacent network element, the job of the physical layer is to move the individual bits within the frame from one node to the next. The protocols in this layer are again link dependent, and further depend on the actual transmission medium of the link (for example, twisted-pair copper wire, single-mode fibre optics). For example, Ethernet has many physical layer protocols: one for twisted-pair copper wire, another for coaxial cable, another for fibre, and so on. In each case, a bit is moved across the link in a different way.

GOTO TOP

Internet History

Development and Demonstration of Early Packet Switching Principles: 1961-1972

The fields of computer networking and today's Internet trace their beginnings back to the early 1 960s, a time at which the telephone network was the world's dominant communication network. Given the increasing importance (and great expense) of computers in the early 1960s and the advent of timeshared computers, it was perhaps natural (at least with perfect hindsight!) to consider the question of how to hook computers together so that they could be shared among geographically distributed users. The traffic generated by such users was likely to be 'bursty' -intervals of activity, such as the sending of a command to a remote computer, followed by periods of inactivity while waiting for a reply or while contemplating the received response.

Three research groups around the world, all unaware of the others' work, began inventing the notion of packet switching as an efficient and robust alternative to circuit switching. The first published work on packet-switching techniques was that of Leonard Kleinrock, at that time a graduate student at MIT. Using queuing theory, Kleinrock's work

Things to Remember:

1961: Kleinrock - queuing theory shows effectiveness of packet-switching

1964: Baran - packet-switching in military nets

1967: ARPAnet conceived by Advanced Research Projects Agency

1969: First ARPAnet node operational

1972:

ARPAnet demonstrated publicly

elegantly demonstrated the effectiveness of the packet-switching approach for bursty traffic sources. In 1964, Paul Baran at the Rand Institute had begun investigating the use of packet switching for secure voice over military networks, and at the National Physical Laboratory in England, Donald Davies and Roger Scantlebury were also developing their ideas on packet switching.

NCP (Network Control Protocol) first host-host protocol

First e-mail program

ARPAnet has 15 nodes

The work at MIT, Rand, and NPL laid the foundations for today's Internet. But the Internet also has a long history of a let's-build-it-and-demonstrate-it attitude that also dates back to the early 1960s. J C R Licklider and Lawrence Roberts, both colleagues of Kleinrock's at MIT, went on to lead the computer science program at the Advanced Research Projects Agency (ARPA) in the United States. Roberts published an overall plan for the so-called ARPAnet, the first packet-switched computer network and a direct ancestor of to day's public Internet.

The early packet switches were known as interface message processors (IMPs) and the contract to build these switches was awarded to the BBN Company. On Labour Day in 1969, the first IMP was installed at UCLA under Kleinrock's supervision, with three additional IMPs being installed shortly thereafter at the Stanford Research Institute (SRI), UC Santa Barbara, and the University of Utah. The fledgling precursor to the Internet was four nodes large by the end of 1969. Kleinrock recalls the very first use of the network to perform a remote login from UCLA to SRI, crashing the system.

By 1972, ARPAnet had grown to approximately 15 nodes, and was given its first public demonstration by Robert Kahn at the 1972 International Conference on Computer Communications. The first host-to-host protocol between ARPAnet end systems known as the network-control protocol (NCP) was completed [RFC 001]. With an end-to-end protocol available, applications could now be written. The first e-mail program was written by Ray Tomlinson at BBN in 1972.

GOTO TOP

Internetworking, and New and Proprietary Networks: 1972-1980

The initial ARPAnet was a single, closed network. In order to communicate with an ARPAnet host, one had to actually be attached to another ARPAnet IMP. In the early to mid 1970s, additional packet-switching networks besides ARPAnet came into being:

- ALOHAnet, a microwave network linking together universities on the Hawaiian islands;
- Telenet, a BBN commercial packet-switching network based on ARPAnet technology;
- Tyrnnet;
- Transpac, a French packet-switching network.

Things to Remember:

1970: ALOHAnet satellite in Hawaii

1973: Metcalfe's PhD thesis proposes Ethernet

1974: Cerf and Kahn - architecture for interconnecting networks

Late 70s: Proprietary architectures: DECnet, SNA, XNA

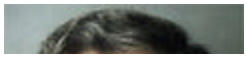
Late 70s: Switching fixed lenght packets (ATM precursor)

1979: ARPAnet has 200 nodes


Robert Metcalfe

The number of networks was beginning to grow. In 1973, Robert Metcalfe's PhD thesis laid out the principle of Ethernet, which would later lead to a huge growth in so-called local area networks (LANs) that operated over a small distance based on the Ethernet protocol.

Once again, with perfect hindsight one might now see that the time was ripe for developing an encompassing architecture for connecting networks together. Pioneering work on interconnecting networks, once again under the sponsorship of DARPA (Defense Advanced Research Projects Agency) -in essence creating a network of networks -was done by Vinton Cerf and Robert Kahn. The term 'internetting' was coined to describe this work.

These architectural principles were embodied in the TCP protocol. The

early versions of TCP, however, were quite different from today's TCPs. The early versions of TCP combined a reliable in-sequence delivery of data via end-system retransmission (still part of today's TCP) with forwarding functions (which today are performed by IP). Early experimentation with TCP, combined with the recognition of the importance of an unreliable, non-flow-controlled end-to-end transport service for applications such as packetised voice, led to the separation of IP out of TCP and the development of the UDP protocol. The three key Internet protocols that we see today -TCP, UDP, and IP -were conceptually in place by the end of the 1970s.

In addition to the DARPA Internet-related research, many other important networking activities were underway. In Hawaii, Norman Abramson was developing ALOHAnet, a packet-based radio network that allowed multiple remote sites on the Hawaiian Islands to communicate with each other.

The ALOHA protocol was the first so-called multiple-access protocol, allowing geographically distributed users to share a single broadcast communication medium (a radio frequency). Abramson's work on multiple-access protocols was built upon by Metcalfe and Boggs in the development of the Ethernet protocol for wire-based shared broadcast networks; interestingly, Metcalfe and Boggs' Ethernet protocol was motivated by the need to connect multiple PCs, printers, and shared disks together.

Things to Remember:

Cerf and Kahn's Internetworking Principles:

Minimalism, autonomy - no internal changes required to interconnect networks

Best effor service model

Stateless routers

Decentralized control

Twenty-five years ago, well before the PC revolution and the explosion of networks, Metcalfe and Boggs were laying the foundation for today's PC LANs. Ethernet technology represented an important step for internetworking as well. Each Ethernet local area network was itself' a network, and as the number of LANs proliferated, the need to internetwork these LANs together became increasingly important.

GOTO TOP

Metcalfe's Original Conception of the Ethernet


Robert Metcalfe

In addition to the DARPA internetworking efforts and the Aloha/Ethernet multiple-access networks, a number of companies were developing their own proprietary network architectures. Digital Equipment Corporation (Digital) released the first version of the DECnet in 1975, allowing two PDP-ll minicomputers to communicate with each other. DECnet has continued to evolve since then, with significant portions of the OSI protocol suite being based on ideas pioneered in DECnet. Other important players during the 1970s were Xerox (with the XNS architecture) and IBM (with the SNA architecture). Each of these early networking efforts would contribute to the knowledge base that would drive networking in the 80s and 90s.

It is important to note here that in the 1980s (and even before), researchers such as [Fraser 1983, 1993] and [Turner 1986] were also developing a competitor technology to the Internet architecture. These efforts have contributed to the development of the ATM architecture, a connection-oriented approach based on the use of fixed-size packets, known as cells.

GOTO TOP

A Proliferation of Networks: 1980-1990

By the end of the 1970s, approximately 200 hosts were connected to the ARPAnet. By the end of the 1980s the number of hosts connected to the public Internet, a confederation of networks looking much like today's Internet, would reach 100,000. The 1980s would be a time of tremendous growth.

Much of the growth in the early 1980s resulted from several distinct efforts to create computer networks linking universities together. BITnet (because it's their network) provided e-mail and file transfers among several universities in the Northeast. CSNET (computer science network) was formed to link together university researchers without access to ARPAnet. In 1986, NSFNET was created to provide access to NSF-sponsored supercomputing centres. Starting with an

Things to Remember:

1983: deployment of TCP/IP

1982: SMTP email protocol defined

1983: DNS defined for name-to-IP address translation

1985: FTP protocol defined

initial backbone speed of 56 Kbps, NSFNET's backbone would be running at 1.5 Mbps by the end of the decade, and would be serving as a primary backbone linking together regional networks.

1988: TCP congestion control

In the ARPAnet community, many of the final pieces of today's Internet architecture were falling into place. January 1, 1983, saw the official deployment of TCP/IP as the new standard host protocol for ARPAnet (replacing the NCP protocol). The transition [RFC 801] from NCP to TCP/IP was a 'flag day' type event -all hosts were required to transfer over to TCP/IP as of that day. In the late 1980s, important extensions were made to TCP to implement host-based congestion control. The Domain Name System, used to map between a human-readable Internet name (for example, gaia.cs.umass.edu) and its 32-bit IP address, was also developed [RFC 1034].

In parallel with this development of the ARPAnet (which was for the most part a United States effort), in the early 1980s the French launched the Minitel project, an ambitious plan to bring data networking into everyone's home. Sponsored by the French government, the Minitel system consisted of a public packet-switched network (based on the X.25 protocol suite, which uses virtual circuits), Minitel servers, and inexpensive terminals with built-in low speed modems.

The Minitel became a huge success in 1984 when the French government gave away a free Minitel terminal to each French household that wanted one. Minitel sites included free sites -such as a telephone directory site -as well as private sites, which collected a usage- based fee from each user. At its peak in the mid 1990s, it offered more than 20,000 different services, ranging from home banking to specialized research databases. It was used by over 20% of France's population, generated more than $1 billion each year, and created 10,000 jobs.

The Minitel was in a large proportion of French homes 10 years before most Americans had ever heard of the Internet. It still enjoys widespread use in France, but is increasingly facing stiff competition from the Internet.

Things to Remember:

New National Networks: Csnet, BITnet, NSFnet, Minitel

100,000 hosts connected to confederation of networks

GOTO TOP

Commercialization and the Web: the 1990s

The 1990s were ushered in with two events that symbolized the continued evolution and the soon-to-arrive commercialization of the Internet. First, ARPAnet, the progenitor of the Internet ceased to exist. MILNET and the Defense Data Network had grown in the 19808 to carry most of the US Department-of-Defense-related traffic and NSFnet had begun to serve as a backbone network connecting regional networks in the United States and national networks overseas. In 1991, NSFNET lifted its restrictions on use of NSFNET for commercial purposes. NSFNET itself would be decommissioned in 1995, with Internet backbone traffic being carried by commercial Internet service providers.

The main event of the 1990s, however, was to be the release of the World Wide Web, which brought the Internet into the homes and businesses of millions and millions of people worldwide. The Web also served as a platform for enabling and deploying hundreds of new applications, including online stock trading and banking, streamed multimedia services, and information retrieval services.


Tim Berners-Lee

The Web was invented at CERN by Tim Berners-Lee in 1989-1991, based on ideas originating in earlier work on hypertext frOD1 the] 940s by Bush and since the 1960s by Ted Nelson. Berners-Lee and his associates developed initial versions of HTML, HTTP, a Web server, and a browser - the four key components of the Web. The original CERN browsers only provided a line-mode interface.

Around the end of 1992 there were about 200 Web servers in operation, this collection of servers being the tip of the iceberg for what was about to come. At about this time several researchers were developing Web browsers with GUI

Things to Remember:

Early 1990s: ARPAnet decommisioned

1991: NSF lifts restrictions on commercial use of NSFnet (decommisioned 1995)

Early 1990s: WWW

- Hypertext [Bush 1945, Nelson 1960s]
- HTML, http: Berners-Lee
- 1994: Mosaic, later Netscape
- Late 1990s: commercialization of WWW

Things to Remember:

Late 1990s:

- Estimated 50 million

interfaces, including Marc Andreesen, who led the development of the popular GUI browser Mosaic for X. Andreesen and his colleagues released an alpha version of his browser in 1993, and in 1994 he and James Baker formed Mosaic Communications, which later became Netscape Communications Corporation. By 1995, university students were using Mosaic and Netscape browsers to surf" the Web on a daily basis. At about this time companies -big and small -began to operate Web servers and transact commerce over the Web. In 1996, Microsoft got into the Web business in a big way though lately realizing the huge business potential of the Internet

computers on Internet

- Estimated 100 million+ users
- Backbone links running at 1 Gbps

During the 1990s, networking research and development also made significant advance. The technical community struggled with the problems of defining and implementing an Internet service model for traffic requiring real-time constraints, such as continuous media applications. The need to secure and manage Internet infrastructure also became of paramount importance as e-commerce applications proliferated and the Internet became a central component of the world's telecommunications infrastructure.

GOTO TOP

Read Chapter 1 of **Computer Networking: A Top Down Approach Featuring the Internet, 2nd edition**. Jim Kurose, Keith Ross Addison-Wesley, July 2002.

Recommended Links

IEEE History Center http://www.ieee.org/organizations/history_center/oral_histories/comsoc_oh.html.
Oral Histories that have been collected to commemorate the 50th Anniversary of the IEEE Communications Society. A number of interesting interviews with pioneers in the field.

International Engineering Consortium: Web ProForum Tutorials http://www.iec.org/online/tutorials/
More than 150 tutorials on communications and networking topics, with a focus on cutting edge technology. The tutorials vary in terms of their technical depth, but many are outstanding, and all are extremely well-written and very readable. This is the first place we look when looking for an on-line survey or tutorial.

Broadband: Bringing home the bits http://www.nap.edu/html/broadband
Extensive report on the importance and future of residential broadband access from the Computer Science And Telecommunications Board, National Research Council, January 2002

Internet Economics http://china.si.umich.edu/telecom/net-economics.html
Comprehensive index for resources relating to Internet economics, including regulation and pricing.

Webopedia http://www.pcwebopaedia.com
Online dictionary for computer and Internet technology

traceroute.org http://www.traceroute.org
As discussed in Section 1.6, Traceroute provides routes and packet delays between pairs of hosts in the Internet. This site gives you direct access to hundreds of source hosts from which you can trace routes to arbitrary destination hosts. Choose a country, a source host in that country, and any destination host -- then see how the packets weave their way through the Internet.

Internet Engineering Task Force (IETF) http://www.ietf.org
The IETF is an open international community concerned with the development and operation of the Internet and its architecture. The IETF was formally established by the Internet Architecture Board (IAB), http://www.isi.edu/iab, in 1986. The IETF meets three times a year; much of its ongoing work is conducted via mailing lists by working groups. Typically, based upon previous IETF proceedings, working groups will convene at meetings to discuss the work of the IETF working groups. The IETF is administered by the Internet Society, http://www.isoc.org, whose Web site contains lots of high-quality, Internet-related material.

Henning Schulzrinne's Internet Technical Resources http://www.cs.columbia.edu/~hgs/internet
Henning Schulzrinne has an extensive - although not always current - index of online resources for the Internet.

The Association for Computing Machinery (ACM) http://www.acm.org
A major international professional society that has technical conferences, magazines, and journals in the networking area. The ACM Special Interest Group in Data Communications (SIGCOMM), http://www.acm.org/sigcomm, is the group within this body whose efforts are most closely related to networking

The Institute of Electrical and Electronics Engineers (IEEE) http://www.ieee.org
The other major international professional society that has technical conferences, magazines, and journals in the networking area. The IEEE Communications Society, http://www.comsoc.org, and the IEEE Computer Society, http://www.computer.org, are the groups within this body whose efforts are most closely related to networking.

The SETI@home Project http://setiathome.ssl.berkeley.edu
As discussed in Section 1.2, the SETI@home project is a scientific experiment that uses Internet-connected computers to search for extraterrestrial intelligence. You can download the SETI program directly from this site.

Nerds 2.0.1 A Brief History of the Internet http://www.pbs.org/opb/nerds2.0.1

This is the Web site for the highly entertaining and informative PBS video on the history of the Internet. The PBS video, Triumph of the Nerds, about the history of personal computers, is also recommended.

Leonard Kleinrock's Personal History of the Internet http://www.lk.cs.ucla.edu/LK/Inet/birth.html
Professor Leonard Kleinrock made numerous important contributions to Internet technology and to the field of computer networking. This page provides his own interesting and highly entertaining description of the early history of the Internet.

The DSL Forum http://www.dslforum.org
DSL Forum is a consortium of nearly 250 leading industry players covering telecommunications, equipment, computing, networking and service provider companies. The site is rich in information about developments in digital subscriber loop and broadband access to the home.

Cable-modems.org http://www.cable-modems.org
This site has many tutorials on cable modems, hybrid fiber-coax, and related topics. Also includes reviews of cable modem products

GOTO TOP