An Introduction to Information Networks

The learning goals for this chapter are as follows:

- Understand the structure of the worldwide information superhighway, commonly known as the Internet, as well as the various components that are inherent to its operation.
- Explore the numerous ways in which the Internet can be accessed through a variety of networks and transmission media
- Learn the composition of the network core that forms the Internet backbone and the organizations that support its continued development
- Learn the difference between packet switching and circuit switching, as well as the ramifications of each
- Understand the layers of the protocol stack that are used to support the interaction of computers connected to the Internet
- Learn the operations performed by the various layers of the protocol stack and the manner in which they affect the data, traveling in packets
- Obtain an overview of the role of security in the Internet
- Learn the manner in which the Internet has developed throughout its history

I.1 INTRODUCTION

There are three primary goals for this book: (1) understand the many facets and ramifications of the Internet and the wide spectrum of applications that it affords, (2) obtain a thorough grasp of computer networks, the various structures and myriad ways in which they are applied, and finally (3) learn how to apply the latest advances in Internet security in order to protect the networks and the large variety of applications running on them. Every attempt will be made to present the material in an easily understandable fashion. As such, the book will contain a plethora of aids that support the rapid assimilation of the material so that the reader can apply it as quickly as possible.

The goals of this text will be accomplished through a systematic progression of material that supports a rapid learning process. The book will be divided into parts, each of which will consist of several chapters. The different parts and the subjects that will be addressed in each are listed in Table I.1.

In this initial chapter we begin to lay the groundwork for our analysis of the concepts that form the foundation of our study of the Internet and the plethora of ways in which they can be employed. We will provide an overview of the Internet architecture and then zoom in on the access networks with which Internet users are typically familiar, together with the backbone that supports them.

The Internet contains a constant flow of information and this information is contained in packets. The manner in which these packets are switched is fundamental to the operation of the Internet. The Internet protocols, software, hardware, commands and similar functions that support packet switching are modularized in what are called protocol stacks and each layer of the stack performs a specific and vital function. These functions will be discussed in detail as we progress through the book. As will be indicated later, packet switching is a best effort delivery

TABLE I.1 The Six Parts of This Book

Introduction	The Internet architecture, together with the various protocols, protocol layers and service models
Part 1	The most important Internet applications and the methods used to develop them
Part 2	The network edge consisting of hosts, access networks, local area networks (LANs) and the various physical media used in conjunction with the Physical and Link Layers; including multiple layer (layer 2 and layer 3) switches and their design
Part 3	The network core, with all the elements that reside there such as packet/circuit switches, routers and the Internet backbone
Part 4	The transport and management of datagrams with the attendant issues of loss, delay, flow and congestion control
Part 5	Cybersecurity mechanisms and their application
Part 6	Emerging technologies

and suffers from the fact that delay jitter is inherent in its operation. In contrast, circuit switching does not have this drawback and therefore is best for voice and video. Packet switching requires the use of protocols to reserve bandwidth and resources in order to mimic circuit-switching operations.

Finally, a basic overview of various types of malware will be presented together with the various security systems, containing such things as firewalls, intrusion detection systems and the like. Network security is a fundamental issue and plays a vital role in the construction and operation of viable computer networks.

Given this conceptual view of the material to follow, let us now begin our presentation by first providing a global picture of the Internet.

I.2 THE INTERNET ARCHITECTURE

I.2.1 A HIERARCHICAL STRUCTURE

A global view of the Internet architecture is shown in Figure I.1. It is in essence a network of networks with a hierarchical structure and is reminiscent of the plain old telephone service (POTS) in which a call went from your phone to a central office by wire, then perhaps to a regional office by radio and finally cross-country by microwave then back down through a similar path to the receiver. The path through the Internet is similar in which a message from one host, e.g., PC, smartphone, etc. to another traverses a similar path, e.g., from sender to Regional ISP to Global ISP to Regional ISP to receiver. In this case, the figure indicates the path that would be traversed by sending a message from one host, e.g., PC, smartphone, etc, to another. The path into the Internet backbone could be wired, e.g., Digital Subscriber Line (DSL), Hybrid Fiber Coax (HFC), etc. or wireless. The backbone itself consists of global Internet Service Providers (ISPs) and several regional ISPs that are all interconnected to provide a path from sender to receiver. The communication path may typically contain a variety of switches and routers that facilitate and direct the flow of information through the network.

A moment's reflection indicates that the Internet is used to connect billions of hosts throughout the world running a wide spectrum of applications. It is absolutely mindboggling to envision the traffic that exists on this ubiquitous network at any given instant. Hosts, e.g., clients or servers, are connected through communication links and information passes through routers, switches and access points on a pathway of such things as fiber, copper or radio. The communication links, regardless of whether they are wired or wireless, are defined by a transmission rate and bandwidth. Access networks are used to connect a host or Local Area Network (LAN) to the Internet. Routers connect local area networks, generate routing tables and forward packets of data on their path from source to destination. The Internet backbone is basically a group of routers interconnected by optical fiber as well as DNS servers containing infrastructure name servers, such as root Domain Name Servers (DNSs) employed for naming. The remaining com-

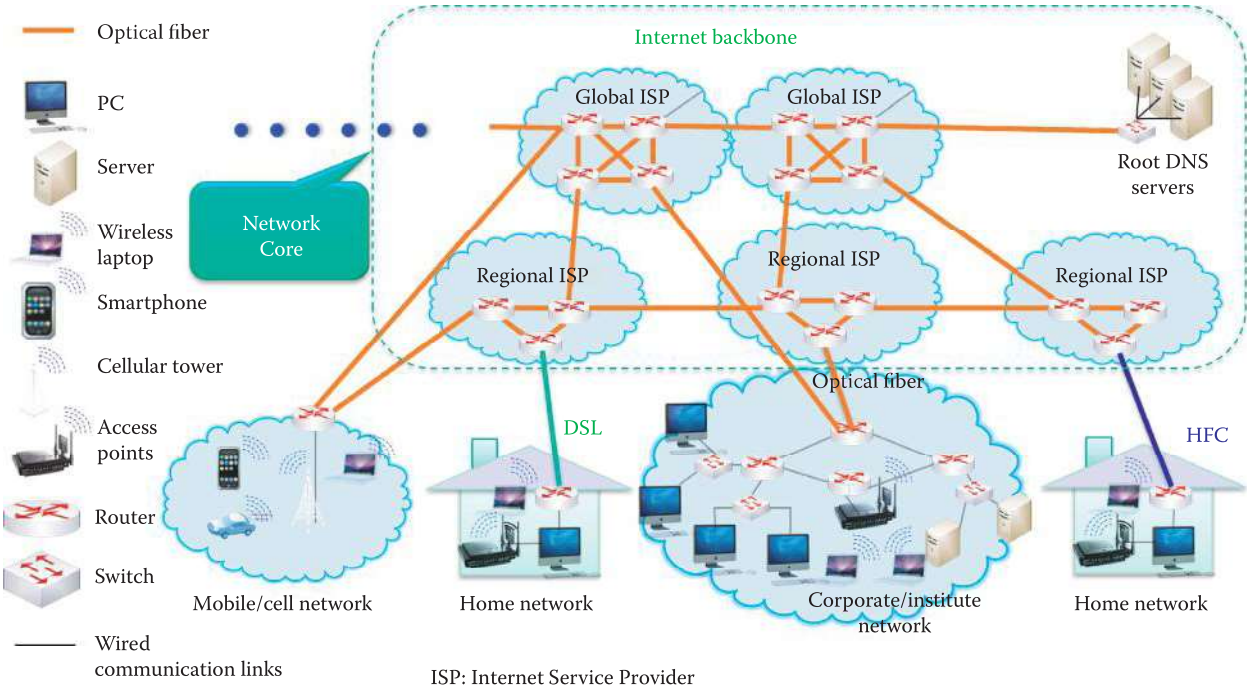


FIGURE I.1 The Internet architecture.

ponents in the Internet structure that lie outside the network core, are simply access networks as indicated in Figure I.1.

As shown in Figure I.1, the Internet is essentially a network of interconnected networks. There is a hierarchical structure in this enormous mass. From a top-down view the Internet consists of a backbone that connects Internet Service Provider (ISP) backbones; the ISP backbones connect the backbones of various organizations; an organization's backbone is used to connect LANs; and finally, the LANs connect the hosts that are running such things as HyperText Transmission Protocol (HTTP) or mail.

I.2.2 INTERNET STANDARDS AND THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN)

Given the enormous number of players and the phenomenal amount of information in play at any given time, clearly there must be standards that control the use of the Internet and these standards are listed in what are called Requests For Comments (RFCs) and the organization that oversees this business is the Internet Engineering Task Force (IETF) [1]. All the RFCs can be downloaded free at rfc-editor.org; however, references are provided for them as they are encountered in this text.

As indicated in Figure I.1, the network edge (or access networks) consists of hosts, i.e., servers and clients, and the various applications that are running in the network, e.g., HTTP, mail and the like as well as access links. The network core is composed of edge routers that connect an organization/ISP to the Internet, and these routers are typically interconnected with fiber. The access networks that are present may be either wired, or wireless, communication links.

The internal structure of the Internet Corporation for Assigned Names and Numbers (ICANN) [2] is shown in Figure I.2. Of particular interest is the Internet Engineering Task Force (IETF), which is the standards body for the organization and controls the standards under which the development of the Internet proceeds. The funding for ICANN is obtained through the collection of registration fees from the various domains, which include .com, .net, .uk, .cn, etc. These fees support ICANN in its efforts to provide various services including a DNS database for all Internet users.

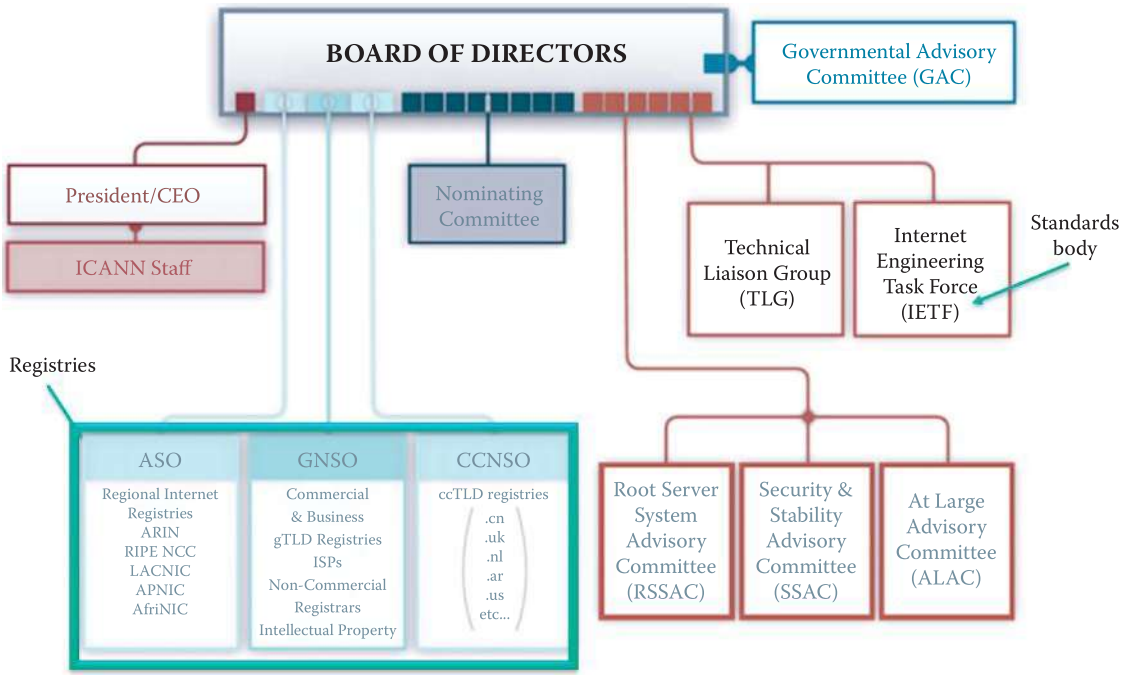


FIGURE I.2 The Internet Corporation for Assigned Names and Numbers (ICANN).

I.3 ACCESS NETWORKS

Given the massive configuration of the Internet, let us now examine the manner in which various hosts of any kind connect into this structure. An individual, home network or business network, e.g., local area network (LAN) can be considered a small network or subnet. The Internet uses a gateway, also known as an edge router, as the vehicle for entrance into the hierarchical network. Such an arrangement is shown in Figure I.3.

The Internet has become an integral part of most people's lives, and therefore households everywhere have Internet access. The point-to-point access between a residence and an ISP can be obtained in a variety of ways. For example, residential Internet access can be obtained via a dialup modem, a digital subscriber line (DSL), a cable modem, fiber in the loop, broadband over a power line, and broadband wireless such as a Wireless Metropolitan Area Network (WiMAX) or satellite. Let's examine each of these in some detail.

A dialup connection to the Internet will operate at a speed of up to 56 Kbps. If a poor quality line is involved, the speed may be less and surfing the Internet can be a slow and tedious process. If compression is employed the speed may reach 320 Kbps. However, surfing the Internet and talking on the phone at the same time are not allowed.

I.3.1 DIGITAL SUBSCRIBER LINES (DSL)

The digital subscriber line is defined by a dedicated physical line between a residential telephone and the telephone company's central office. This line is supplied by the telephone company and is not shared with anyone else. The DSL line speed is controlled by the distance between the phone and the central office, or the telephone company's Digital Subscriber Line Access Multiplexer (DSLAM). The standard for this technology in the U.S. is defined by ANSI T1.413-1998 Issue 2 [3], where ANSI is the American National Standards Institute. This standard defines the upstream rate to be a maximum of 1 Mbps, typically less than 256 Kbps, and the downstream rate to be maximum of 8 Mbps, typically less than 6 M bps. Frequency Division Multiplexing (FDM) can be used with this technology, and in this mode one can surf the Internet and use the phone at the same time. In this mode, the upstream rate is 4 KHz to 50 KHz, the downstream rate is 50 KHz to 1 MHz, while the ordinary telephone employs the range between 0 KHz to 4 KHz.

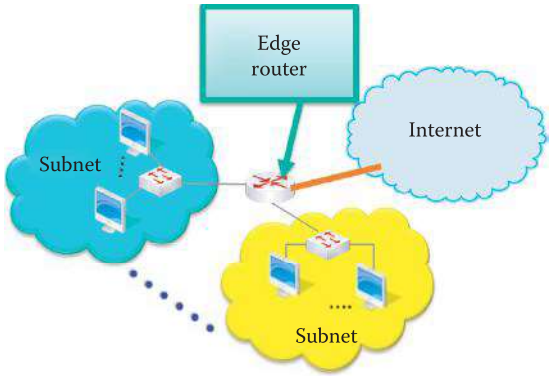


FIGURE I.3 A router with subnet.

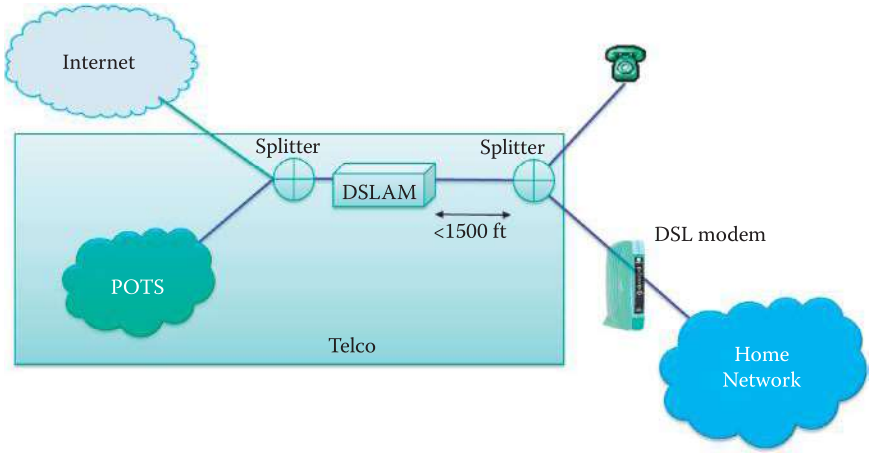


FIGURE I.4 The Digital Subscriber Line's (DSL) function in the network.

The network, shown in Figure I.4, illustrates some of the various components typically connected to the telephone company. The telephone company contains the Plain Old Telephone Service (POTS), the DSLAM and the splitters employed to connect the outside components such as the Internet, with a telephone and/or home network that connects through the DSL modem. It is important to note that the splitters must be less than 1500 feet from the DSLAM.

I.3.2 HYBRID FIBER COAX (HFC)

Most people are familiar with another technology that is employed for residential Internet access and that is the cable modem. The present technology is hybrid fiber coax (HFC), shown in Figure I.5, in which fiber is extended into a neighborhood and then coax is used to connect individual homes. In this manner, a number of homes share a coax cable in order to obtain Internet access. This technology deployed by the TV cable companies, uses fiber to the neighborhood and coax to the home in order to connect to an ISP router. This HFC technology is deployed by cable companies that supply TV, and this network of coax and fiber connects homes to the ISP router. The standards for this service are called the Data Over Cable Service Interface Specification (DOCSIS) and are developed by Cable Labs. The newest versions are DOCSIS 2.0 and 3.0 [4]. In North America, DOCSIS 2.0 provides for an asymmetric rate of up to 38 Mbps downstream and 27 Mbps upstream, and DOCSIS 3.0 provides for 304 Mbps downstream and 108 Mbps upstream when grouping multiple DOCSIS 2.0 channels. The coax signal downstream in a 6 MHz channel uses a frequency range from 54 to 108 MHz at the lower end and up to 300 MHz, or as much as 1002 MHz, on the upper end. The maximum number of channels is 158 and they are shared by

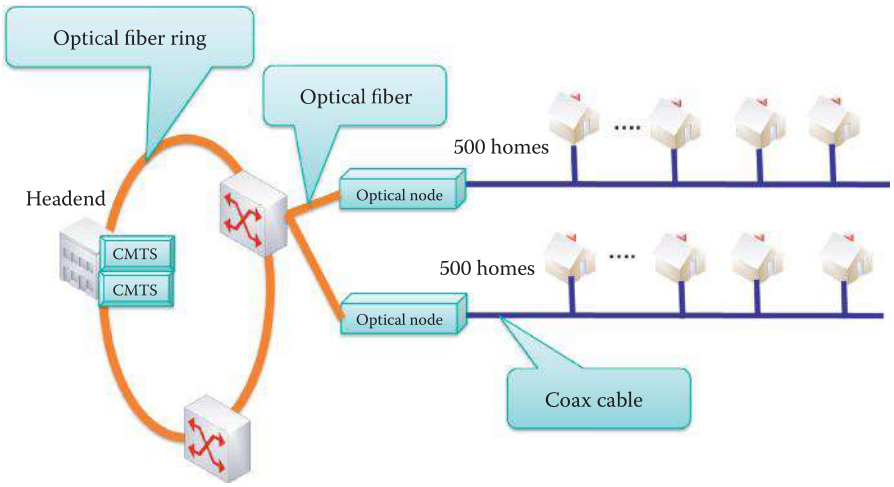


FIGURE I.5 A hybrid fiber coax network.

the neighborhood. In addition, there is a reverse/return path in the frequency range that extends from 5 MHz to either 42 or 85 MHz. More typical rate numbers in this environment are 5 Mbps downstream and 256 Kbps upstream

Figure I.5 illustrates a typical HFC cable network. The headend is the generation/coordination point and it exists on the optical fiber ring. The headend also contains the Cable Modem Termination System (CMTS), which is equivalent to a DSLAM. As the network grows, the CMTS can be upgraded with more downstream and upstream ports. If the HFC network is very large, the CMTS can be grouped into hubs to support a more efficient management of the system. Some users have attempted to override the bandwidth cap and gain access to the full bandwidth of the system, often as much as 38 Mbps, by uploading their own configuration file to the cable modem. This process, called uncapping, is almost always a violation of the Terms of Service agreement. As a result, there is the risk of being dropped from the ISP service. At the optical node, the conversion between light pulses and electrons is done. As indicated, all transmission for some set of homes takes place on the same coax cable.

I.3.3 FIBER IN THE LOOP (FITL)

The ideal manner in which to employ optical fiber is to run it directly from the telephone company's central office to the home, and in this case this Fiber in the Loop (FITL) replaces the POTS, which is composed of copper. A remote Serving Area Interface (SAI) is located in the neighborhood, and an Optical Network Unit (ONU) is located at either the customer's home or premises, i.e., Fiber to the Home (FTTH) or Fiber to the Premises (FTTP). The fiber to the premises is a point-to-multipoint Passive Optical Network (PON). Later versions of this technology are Gigabit PON and Ethernet PON. In early 2008, Verizon deployed Gigabit PON (GPON), and it expanded to more than 800 thousand lines by mid-year. The GPON standard is ITU-T G.984 [5]. Ethernet PON (EPON) enables service providers to deliver up to 100 Mbps full-duplex over a single-mode optical fiber to the premises. The EPON standard is IEEE 802.3ah [6]. China was expected to deploy EPON to approximately 20 million subscribers by the end of 2008.

I.3.4 BROADBAND OVER POWER LINES (BPL) AND HOMEPLUG

Broadband over Power Lines (BPL) is an interesting technology since every home has a power line connection. The power-line Internet, aka Powerband, provides broadband Internet access through ordinary power lines using a BPL modem.

The standard for this technology is IEEE P1901 [7], which was developed in collaboration with the HomePlug Alliance. It includes residential access to the Internet using BPL, typically at

TABLE I.2 Various HomePlug Standards

Standard	Peak data rate
HomePlug Access BPL	A peak data rate of a few Mbps for Internet access
HomePlug 1.0	A peak data rate of 14 Mbps at the physical layer
HomePlug AV	A peak data rate of 200 Mbps at the physical layer
HomePlug AV2	A peak data rate of 600 Mbps at the physical layer
HomePlugGreen PHY	A peak data rate of 10 Mbps at the physical layer for smart meters and smaller appliances with a 256 Kbps minimum effective throughput

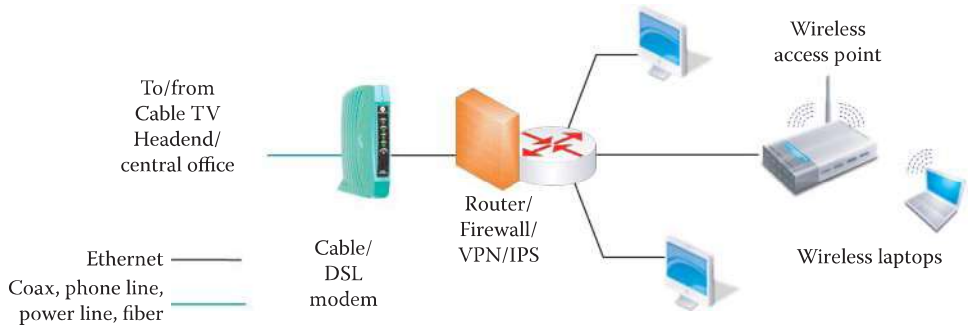


FIGURE I.6 A home network configuration.

10 Mbps, as well as HomePlug AV (HPAV) for an in-home LAN to support Voice over Internet Protocol (VoIP) and video. The HomePlug standards are listed in Table I.2.

This HomePlug AV technology specifies speeds up to 600 Mbps at the physical layer and 500 Mbps at the application layer. Products based on HomePlug AV2 are currently available. Typical rates are much lower, but the upstream and downstream rates are the same. HomePlug AV provides a powerline network with a peak rate of 200 Mbps for video, audio and data. HomePlug AV employs BPL Coexistence through one of two methods: *Coexistence of Services*, and *Coexistence of Technologies*. The *Coexistence of Services* method uses time division multiplexing (TDM) with beacon signaling and messaging to coordinate the in-home and BPL networks, while the *Coexistence of Technologies* method uses frequency division multiplexing (FDM) to permit different technologies to coexist. It is worth noting that the city of Manassas Virginia was the first to deploy a wide-scale BPL service in the U.S in October 2005. They use the MainNet BPL technology and offer a 10 Mbps service for under $30 U.S. per month to approximately 35,000 residents.

The IEEE P1901.2 standard (aka HomePlugGreen PHY) was developed for utility companies and makers of smart meters to support their ability to send data from the smart grid through existing electrical wiring. It is a new narrow band powerline communications standard with a low data rate. Power-line technology is also a viable means of supplying in-vehicle network communication of data, voice, music and video by digital means over a direct current (dc) power line.

I.3.5 A TYPICAL HOME NETWORK

A typical home network may be represented by the configuration shown in Figure I.6. As indicated, the cable TV headend or telephone company central office is connected to the home network by a modem. Powerline or fiber is also applicable in this environment. The router shown in the figure does not perform a routing function, such as, generating a routing table, but is referred to as a router because it performs the network address translation, e.g., it may provide the address 192.168.y.x, as a typical example of a given IP address from the ISP. The router may contain a firewall/virtual private network (VPN) or intrusion prevention system (IPS). The router may also contain a built-in Ethernet switch and a wireless access point.

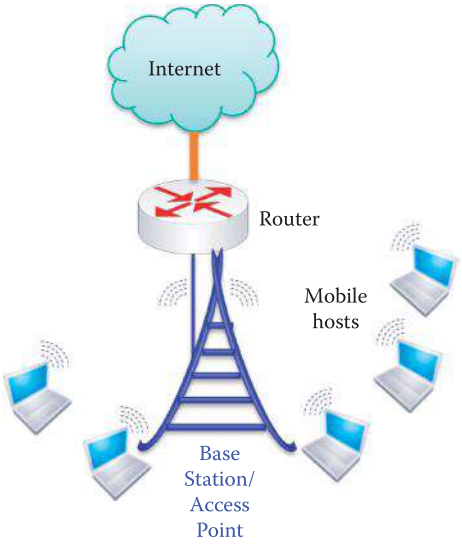


FIGURE I.7 Wireless access networks.

I.3.6 LOCAL AREA NETWORKS (LAN)

As was indicated in Figure I.3, a LAN or subnet containing various hosts is connected to the Internet via an edge router. If the subnet is in an Ethernet LAN, hosts are connected to an Ethernet switch and operate at speeds of 10 Mbps, 100 Mbps, 1 Gbps or 10 Gbps. Each LAN must connect to a router interface in order to connect to the Internet. In the Internet community, the router interface is also called a gateway, and an organization typically uses an asynchronous transfer mode (ATM) leased line via an optical fiber link to connect to an ISP. This router at the edge, i.e., edge router, began as simply a representation for a switch with Ethernet on one end and an ATM line on the other, and thus it is essentially a router connected to a cloud of ATM switches.

I.3.7 WIRELESS ACCESS NETWORKS

As illustrated in Figure I.6 and again in Figure I.7, mobile hosts are connected to the router via an access point or base station. The wireless LANs (WLANs) are governed by the standards 802.11a/b/g (WiFi) [8] operating at between 11 and 54 Mbps, or 802.11n [9] with speeds greater than 100 Mbps. The new standards, 802.11ac and 802.11ad, will operate at rates of up to 1.7 and 7 Gbps, respectively. The wide-area wireless access, provided by the telephone company, has a speed of approximately 1 Mbps over the cellular system, or one can use WiMAX [10] at speeds of 10 Mbps or greater, over a wide area. In free space the signals propagate as radio waves. In this environment, the transmission vehicles are wireless LANs (802.11), 3G wireless (HSDPA and EV-DO) [11][12][13][14], WiMAX and satellite., where HSDPA is High-Speed Downlink Packet Access and EV-DO is Evolution-Data Optimized.

I.3.8 THE TRANSMISSION MEDIA

The transmission media may be physical wires (transmission lines) or free space. The physical links used between the transmitter and receiver are typically a twisted pair (Ethernet 100BASET or 1000BASET), coax (10BASE2) or fiber (100BASEF, 1000BASEX, or 10GBASE-R) [6]. The radio wave propagated in free space suffers more loss than wired transmission media, while fiber is the best medium in terms of data rate and transmission distance.

FIGURE I.8 The Internet eXchange points throughout the world. (Courtesy of https://prefix.pch.net/applications/ixpdir/.)

I.4 THE NETWORK CORE

Having now examined the means employed to access the Internet, let us now turn our attention to the structure that comprises the heart of the Internet, i.e., the network core as illustrated in Figure I.1. The core of the Internet is composed of a set of routers and fiber links, shown in Figure I.1 in orange. The routers work together to determine the most efficient routing path for a packet from source to destination. A distributed algorithm is used that provides the flexibility to adapt to changing conditions, and routing tables are generated and maintained in real time. The ISPs that form the network core interconnect multiple continents. These ISPs are Global ISPs, also known as Tier-1 ISPs, whereas the Regional ISPs are known as Tier-2 ISPs.

I.4.1 INTERNET EXCHANGE POINTS (IXPS)

The Tier-1 ISPs that form the Internet backbone are Verizon, AT&T, Qwest, Level 3 Communications, and the like. These Tier-1 ISPs are interconnected at various access points called Internet eXchange Points (IXPs). There are approximately 300 IXPs in 86 countries. The U.S. has about 88 of them. At these various ISP locations, under bilateral and multilateral agreements, the major ISPs agree to accept traffic from one another and route it to its downstream destination without charge. In addition, the major ISPs also have private agreements between one another in locations where two or more carriers have switching points in close proximity.

Figure I.8 provides a global view of the Internet eXchange Points. The source for this figure is [15]. Clearly, these points have a direct relationship to the population centers of the world.

The IXP typically consists of a centralized Ethernet switching fabric, together with all the supporting infrastructure that permits companies to interconnect with one another at anywhere from 1 Gbps to multiples of 10 Gbps. Because of its strategic importance in the Internet, the ISP carefully monitors all mission critical systems, has a sophisticated fire protection system, and is equipped with ac and dc power, a generator and an uninterruptable power supply. As indicated, these facilities are located throughout the United States and one of them is located at 56 Marietta St, NW, Atlanta, GA 30303.

I.4.2 TIER-1 INTERNET SERVICE PROVIDERS (ISPS)

Tier-1 ISPs typically have backbones that cover the globe. For example, the Verizon backbone is shown in Figure I.9. It is a graphic picture of the manner in which the Internet has developed worldwide. The source for this figure is [16]. Note the relationship between this network and the population centers of the world.

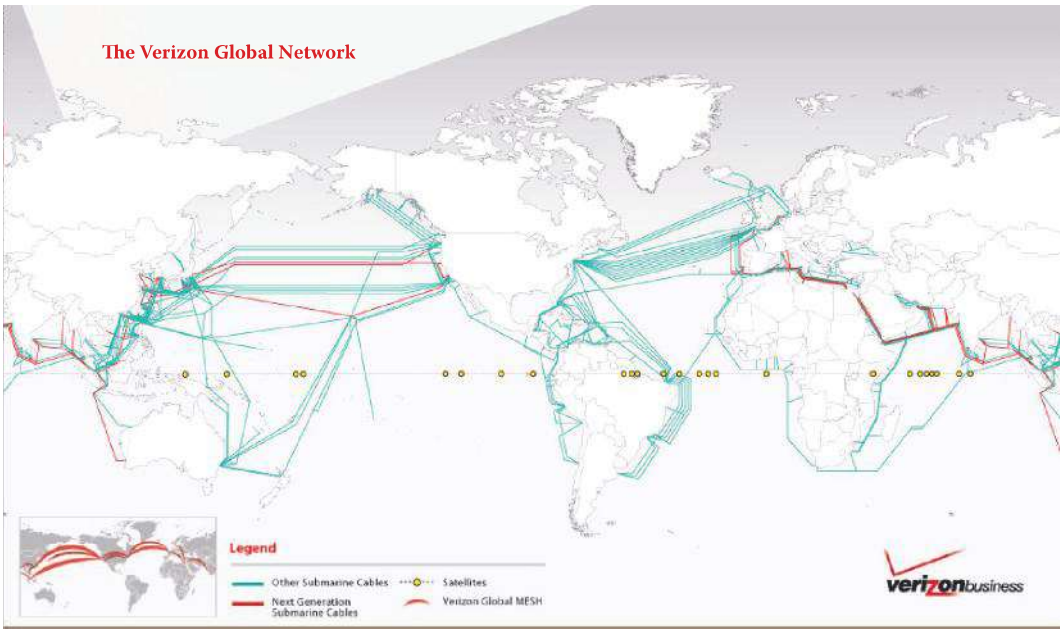


FIGURE I.9 Verizon backbone. (Courtesy of Verizon.)

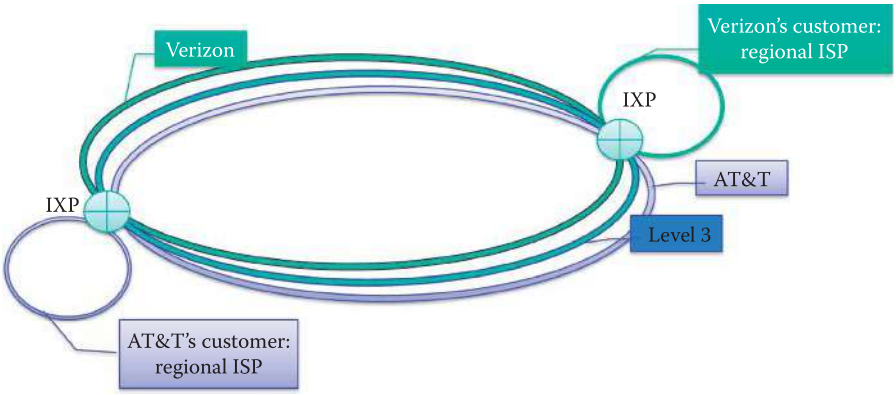


FIGURE I.10 The regional ISP structure.

The manner in which the various regional ISPs connect their customers to the network through an IXP is shown in Figure I.10. In this manner the regional ISPs work in conjunction with other Tier-1 and Tier-2 ISPs to provide the service required by their customer base.

I.4.3 THE INTERNET2 NETWORK

There is a U.S. centric nationwide network that is unique in its mission. This network, known as the Internet2 network [17], shown in Figure I.11, provides the education and research community within the U.S. with a dynamic, innovative and cost-effective hybrid optical and/or packet network. Its backbone network, operating at 10 Gbps and known as the Abilene network, is shown in Figure I.12. In contrast to the Internet2 backbone, which only covers major cities, the network itself covers the entire nation. Internet2 supports research facilities throughout the nation in their development of advanced Internet applications, as well as their enhancement through the deployment of vanguard services, such as IPv6. This IP network, is built over a carrier-class infrastructure, and provides support for the most advanced networking protocols. It is a dynamic circuit network that enables short-term or point-to-point circuits that are established in response to an application in the standard synchronous optical network bandwidth at increments of up to

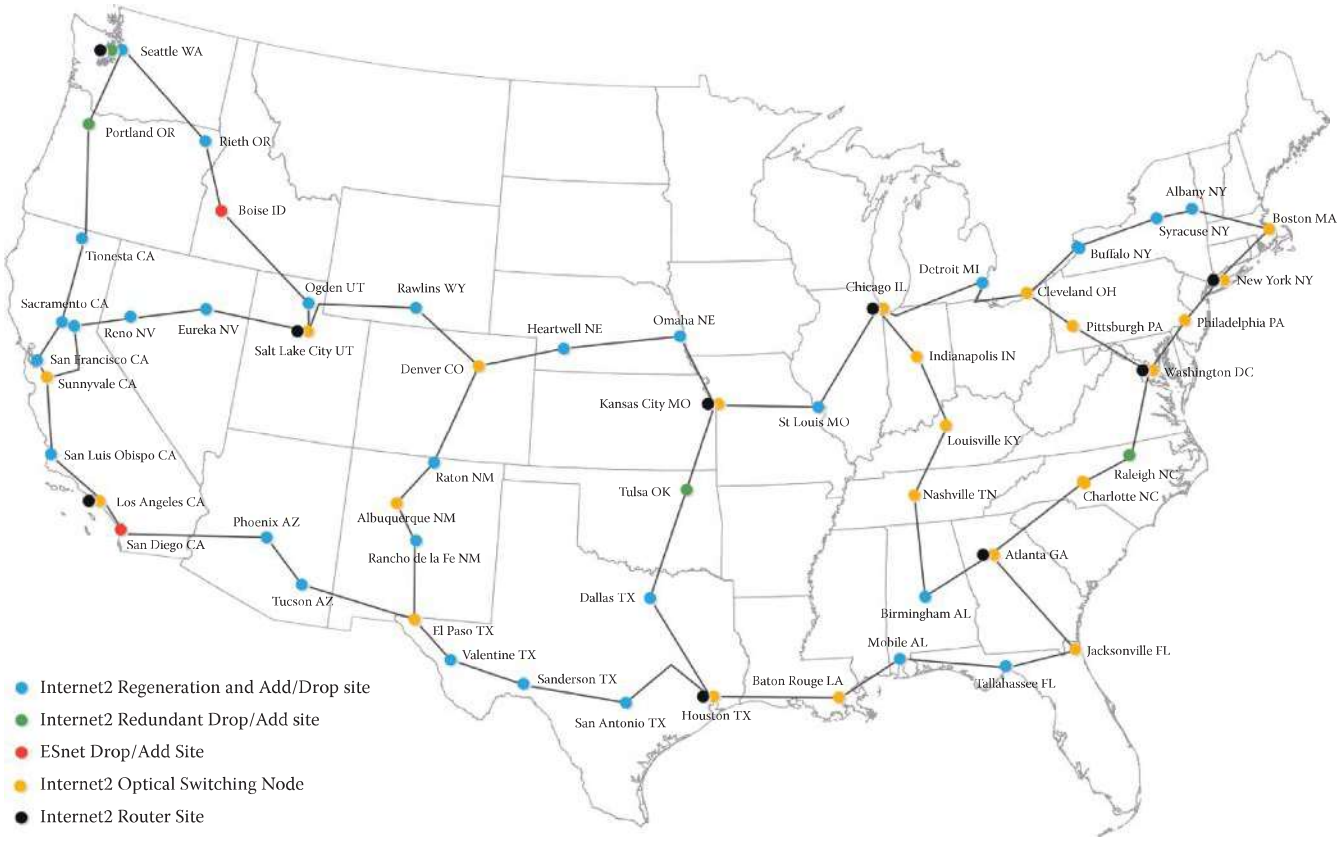


FIGURE I.11 The Internet2 network.

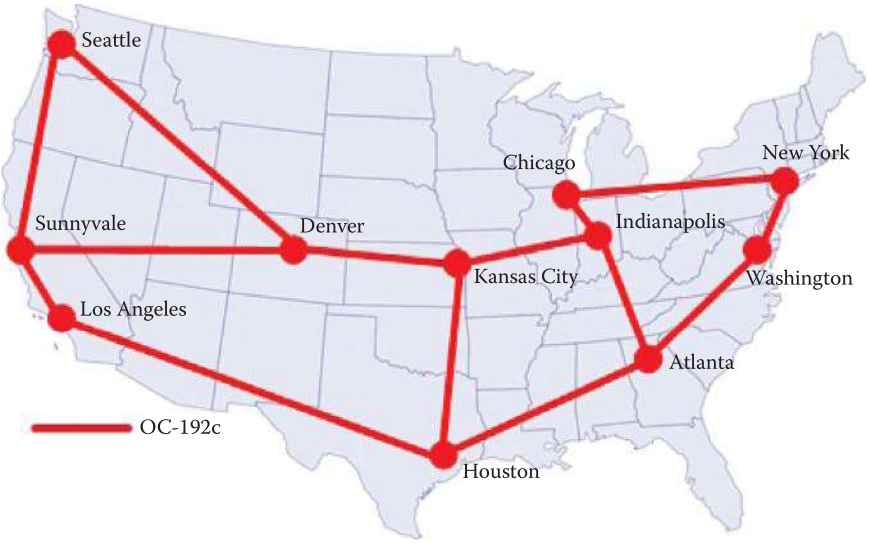


FIGURE I.12 The Internet2 backbone.

10 Gbps. Static networks are provided by either the Internet2-controlled optical infrastructure or the Level 3 Communications network (an ISP network).

Internet2 announced on 11/15/2010 that it will begin deployment of a new, nationwide 100 Gigabit per second (Gbps) Ethernet backbone network using 100 Gbps core routers. The complete deployment of this new network is scheduled for 2013. Internet2 has a long-term partnership with the router/switch vendor, Juniper Networks.

I.5 CIRCUIT SWITCHING VS. PACKET SWITCHING

I.5.1 CIRCUIT SWITCHING

The information organized within the protocols must be switched as it travels from source to destination. The switching function is performed in one of two ways: *Packet switching* or *circuit switching*. In the former case, the header contains the source and destination IP addresses, and the delivery is best effort. Thus, packets may be lost, corrupted or may be delivered out of order. Circuit switching on the other hand uses a dedicated circuit for each call, e.g., when using a dial-up modem, or a virtual circuit, examples of which are the classic IP over Asynchronous Transmission Mode (ATM) or leased lines.

Another way of looking at the difference between circuit switching and packet switching is the following scenario. Consider the difference between a paying airline customer and an airline employee who flies for free. The customer who pays for a round-trip ticket and obtains a reserved seat is analogous to circuit switching, while packet switching is analogous to the airline employee who uses free, open tickets to fly but the seats are not reserved and boarding is only permitted if the seats are available just prior to takeoff.

With circuit switching the end-to-end resources are reserved for the connection, i.e., the connection is established before any data is transferred. Given the dedicated link bandwidth and switch circuit capacity, the performance is guaranteed. Because the resources are dedicated, there is no sharing. So, if Frequency Division Multiplexing (FDM) or Time Division Multiplexing (TDM) is used, a portion of the end-to-end resource will be idle if one of the hosts is not active. Call setup and teardown are required when either modems or constant bit rate (CBR) ATM on leased lines, are used.

Example I.1: The Transmission Delays Inherent in Circuit Switching

For a moment, let's quantify some of the details of circuit switching using an example. Assume that Host A will send 1,000,000 bits to Host B over a switched network. Further assume that the links are T1 lines operating at 1.536 Mbps, each link uses TDM with 24 channels or slots, a single channel is to be used in transmission and 500 milliseconds is needed to establish the end-to-end circuit. Given this data, the time required is

$$[1M/(1.536M/24)] + 500 = 16.125 \text{ seconds.}$$

I.5.2 A COMPARISON OF CIRCUIT SWITCHING WITH PACKET SWITCHING USING STATISTICAL MULTIPLEXING

It is both interesting and instructive to understand the inherent advantages and disadvantages that attend circuit switching and packet switching. In the former case, the advantage is fixed delay jitter, while its main disadvantage is the fact that it cannot fully utilize the bandwidth and network resources that are assigned when a circuit is established. In contrast to circuit switching, packet switching with the use of statistical multiplexing allows heavier traffic for data of a bursty nature than circuit switching over the same links. Under normal demand, packet switching can serve more users, who can only produce bursty traffic, through the use of statistical multiplexing by fully utilizing the bandwidth and network resources that are available. Of course, packet switching is not without its problems either, e.g., packets may be lost and congestion will occur when the bandwidth and network resources are not able to meet the demand. In addition, variable delay jitter accompanies packet switching and thus it is not suitable for voice and video. In order to provide reliable video/voice transport, additional overhead must be paid by packet switch protocols in order to match circuit switching's performance.

Statistical multiplexing (SM), shown in Figure I.13, is an efficient method for packet switching. As indicated, packets from hosts A and B are generated randomly, and if there is no fixed priority, then packets are treated equally based on their order of arrival. Router 1's T1 link bandwidth

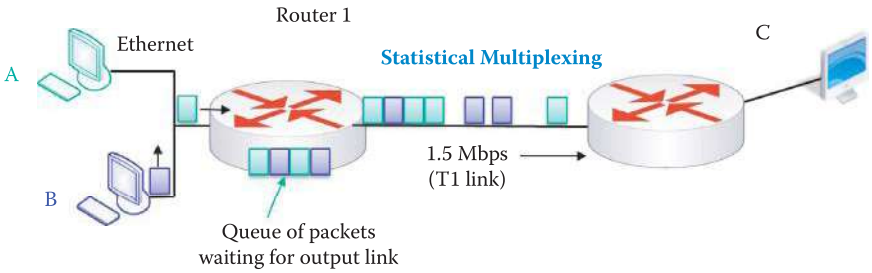


FIGURE I.13 Illustration of statistical multiplexing.

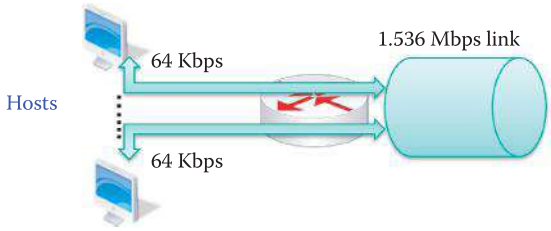


FIGURE I.14 Multiple hosts using a standard T1 link.

is shared by packets from both hosts A and B, and if the T1 link is overwhelmed with packets, they are queued up in the router and await time slots on the output link. This technique stands in sharp contrast to both FDM and TDM with dedicated slots and thus no resource contention.

Example I.2: A Comparison of Packet Switching vs. Circuit Switching Using a T1 Link

As a simple example comparison of packet switching versus circuit switching, consider the network in Figure I.14 where several hosts share a T1 (DS1) link. The T1 link to the Internet is 1.536 Mbps and a standard T1 circuit can be divided into 24 8-bit narrow-band DS0 circuits, sampled 8000 times per second and operating at 64 Kbps when active. In a switching circuit environment, a user is typically assigned a DSO circuit. If it is assumed that the hosts are active on average 20% of the time, then 24 hosts can be circuit-switched since a fixed bandwidth is assigned to each host in spite of the fact that they may exhibit long inactive periods. In reality, when a user is surfing the web, it is impossible to keep a DSO circuit active 100% of the time and inactive periods are a waste of resources.

However, with packet switching (or SM) approximately 120 hosts (24 x 5) or more can statistically be accommodated. SM is based on the average use of bandwidth in determining the number of hosts. No fixed bandwidth is assigned to a host and when a host has inactive periods, other hosts can make effective use of the bandwidth. In this latter case, some hosts may encounter contention and long delays, and thus while packet switching may serve more hosts it does so with some uncertainty due to statistical multiplexing.

Clearly, both packet switching and circuit switching possess some advantages and carry with them some attendant disadvantages. Packet switching is the best technique for bursty data. It provides a best effort delivery and better resource sharing. However, there is the problem of network congestion caused by packet delays in the queue of the routers and packet loss due to queue overflow. Therefore, packet-switching-based protocols carry overhead in order to provide reliable data transfer as well as congestion and flow control. On the other hand, circuit switching is best for voice and video. There is a guaranteed bandwidth as well as guarantees for timing, latency and latency jitter.

Packet switching is widely used for its flexibility and efficiency. For example, HyperTransport, which is an open-standard technology, is being used by Advanced Micro Devices to replace the Front-Side Bus in its multiprocessor interconnect, which includes the graphic processing unit

(GPU) located in the same die as the CPU. Intel's counterpart is called the QuickPath Interconnect. Other examples include Serial Advanced Technology Attachment (SATA), which is a computer bus interface for connecting to hard disk drives, Peripheral Component Interconnect Express bus (PCI Express bus), which is a motherboard-level interconnect to link motherboard-mounted peripheral cards, e.g., a graphics card, and USB.

I.6 PACKET SWITCHING DELAYS AND CONGESTION

I.6.1 PACKET SWITCHING DELAYS

A delay that is inherent in packet switching is the transmission delay. This delay is a direct result of the finite bandwidth of the link employed. The following example illustrates the effect of this delay.

Example I.3: The Transmission Delay Inherent in Packet Switching

With reference to Figure I.15, assume a packet length of L bits and a link rate of R bps. If the link between Router 1 and Router 2 is available, a transmission delay of L/R seconds is encountered in sending one packet over this link. Assuming store and forward routing, i.e., the entire packet must arrive at one router interface before it can be transmitted over the next link, the host-to-host transmission delay = 3L/R; there will also be propagation and other delays. For example, if L = 1000 Mbits, R = 100 Mbps, e.g., Ethernet, then the transmission delay per link is 10 seconds. The total transmission delay is 30 seconds.

As indicated earlier, packets encounter both loss and delays as illustrated in Figure I.16. When the incoming packets rate exceeds the link data rate, the incoming packets must be queued in the buffer, and there is a resultant queuing delay. In addition, if there is no free space in the buffer the incoming packets are dropped, creating a loss.

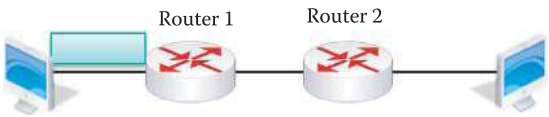


FIGURE I.15 The network used to examine packet transmission latency.

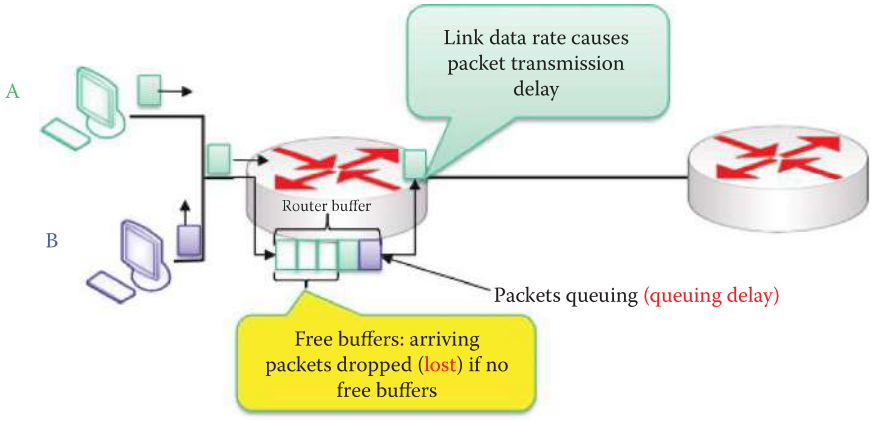


FIGURE I.16 Network illustrating packet loss and delay.

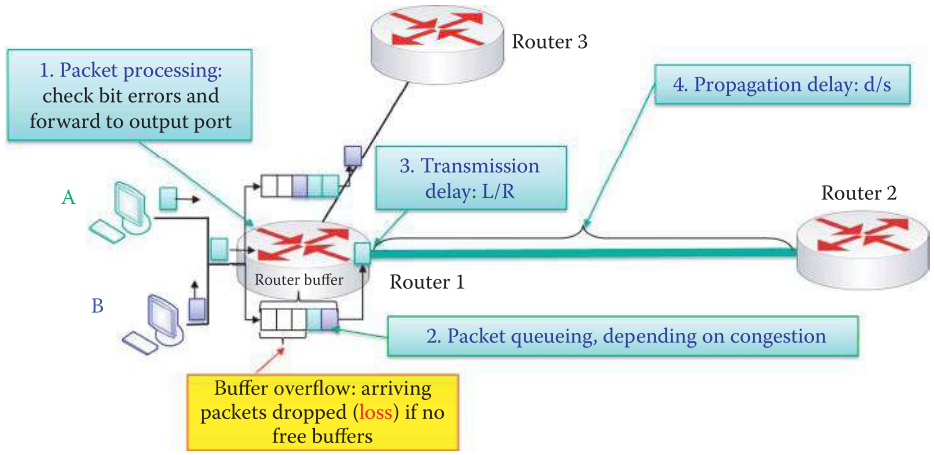


FIGURE I.17 Network used to identify packet delay factors.

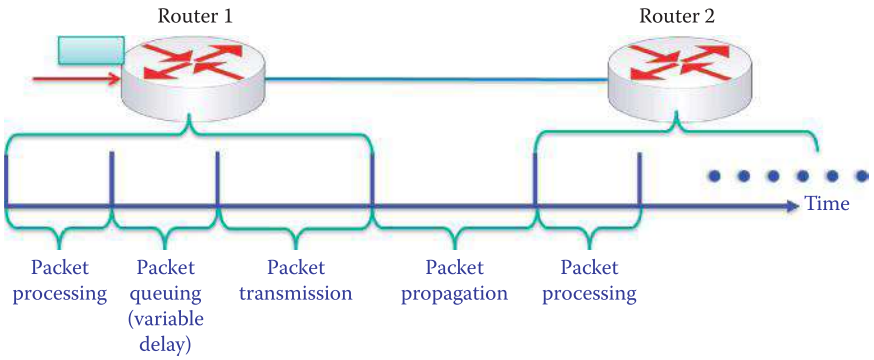


FIGURE I.18 The packet delays for a packet flowing through a router; the queuing delay is variable and depends on the availability of the output link and the other packets in the queue.

There are four delay factors that are encountered with packet switching, and they are labeled in Figure I.17. Thus, the total delay is the sum total of the individual delays. These individual delays are (1) the processing delay at the router input caused by packet processing in which bit errors are checked and the packet is forwarded through the router or into the buffer, (2) the queuing delay caused by packet queuing when congestion is present, (3) the transmission delay (L/R), and (4) the propagation delay (d/s) down the link, where d is the distance down the link and s is the propagation speed. Another view of the packet delays for a packet flowing through a router is shown in Figure I.18. All delays except queuing delay are almost a constant in a router. The queuing delay depends on the availability of the output link and the other packets in the queue.

Packets traveling in the Internet pass through numerous routers, and the routers in today's Internet backbone typically employ multi-threaded network processors or application-specific integrated circuits (ASICs) to perform the forwarding process. Each router processes multiple packets in a parallel fashion and it is impossible to ensure that the output packets have the same order as the input packets in this parallel processing environment. Hence packet switching cannot maintain packet order when a message contains multiple packets.

I.6.2 PACKET LOSS AND DELAY

A primary cause of packet loss is the finite size of the buffer involved. This loss, coupled with the delays outlined earlier, forces the sender to retransmit the data after timeout. The following example provides some insight on these issues.

Example I.4: Packet Processing within a Router and the Associated Delays and Losses

The following example will illustrate the effect that packet delay factors have on packet transmission. In this example, it is assumed that there are two hosts, A and B, each has an infinite buffer, is located zero distance from the first router, and will employ best effort transmission. Host A has 4 packets, A1, A2, A3 and A4 to send, and Host B has 5 packets, B1, B2, B3, B4 and B5, to send. The transmission path to be examined is that from the hosts through Router 1 to Router 2. Both routers have buffer space for 5 packets. The remaining parameters for the example are

Packet length = 7 Kbits
Link rate R = 1 Mbps
Packet processing time = 0.001 s
Propagation speed s = 2×10^8 m/s
Distance between routers d = 2×10^5 m

Therefore,

Propagation delay = d/s = $(2 \times 10^5$ m)/$(2 \times 10^8$ m/s) = 0.001 s
Transmission delay = L/R = (7 Kbits)/(1 Mbps) = 0.007 s

Initially, at time = 0, each host has a packet ready to send as indicated in Figure I.19.

Packet B1 is sent first and takes 0.001 seconds to pass through the router. At time = 0.002 seconds, packet A1 is queued into the buffer, as shown in Figure I.20 and Figure I.21, because packet B1 is still in transmission.

At time = 0.003 seconds, packet B2 is queued into the buffer, as shown in Figure I.21 and Figure I.22, because packet B1 is still in transmission.

As Figure I.22 and Figure I.23 indicate, at time = 0.004 seconds, packet A2 is queued into the buffer.

As indicated in Figure I.24 and Figure I.25, when A3 is queued into the buffer the buffer will be full.

As Figure I.25 indicates, the buffer is full and packet B1 is still in transmission. Therefore, packet B4 is discarded.

Furthermore, since packet B1 will not complete transmission until time = 0.008 seconds (0.001 s for processing and 0.007 s for transmission), packet A4 will also be dropped, as shown in Figure I.26.

Finally, at time = 0.009 seconds, packet B1 has completed transmission to Router 2 and packet B5 is placed in the buffer, as shown in Figure I.27.

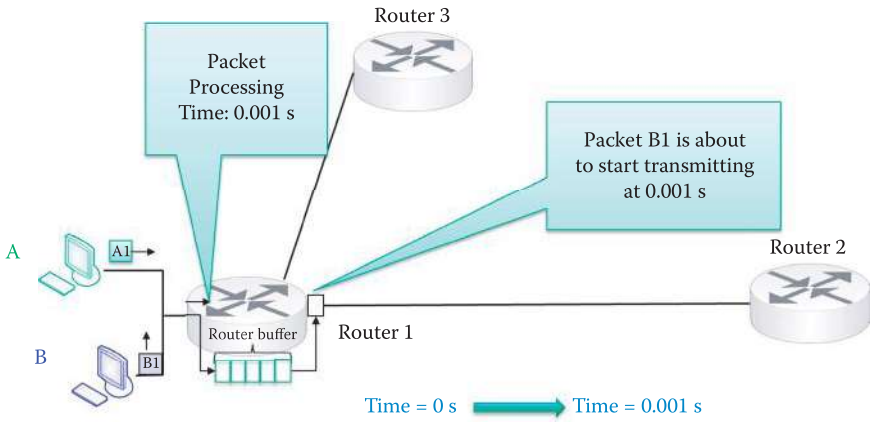


FIGURE I.19 Delay factor example at time 0 s.

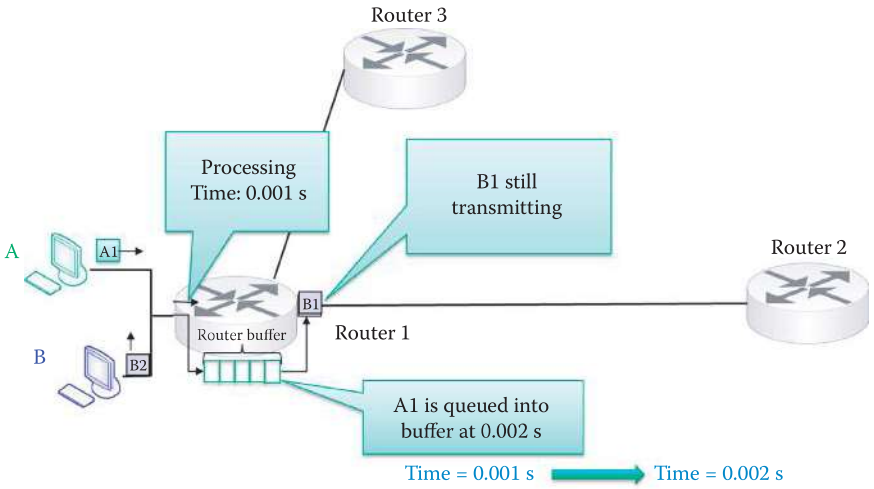


FIGURE I.20 Delay factor example at time 0.001 s.

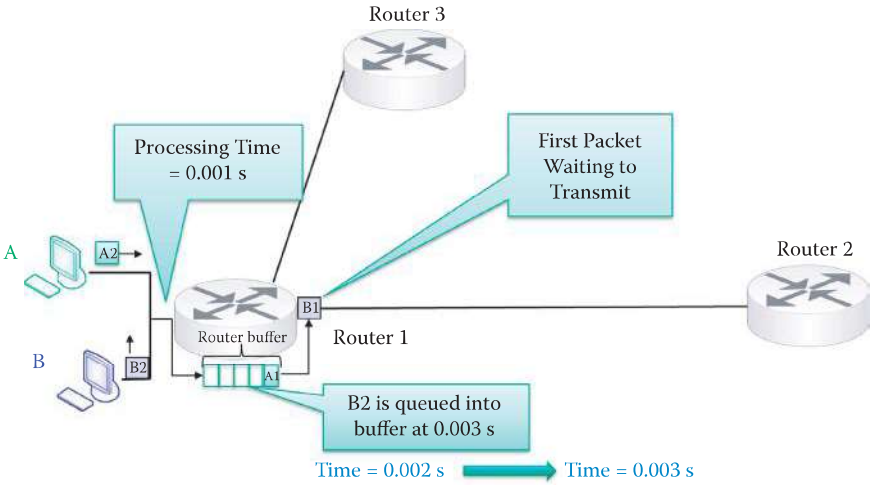


FIGURE I.21 Delay factor example at time 0.002 s.

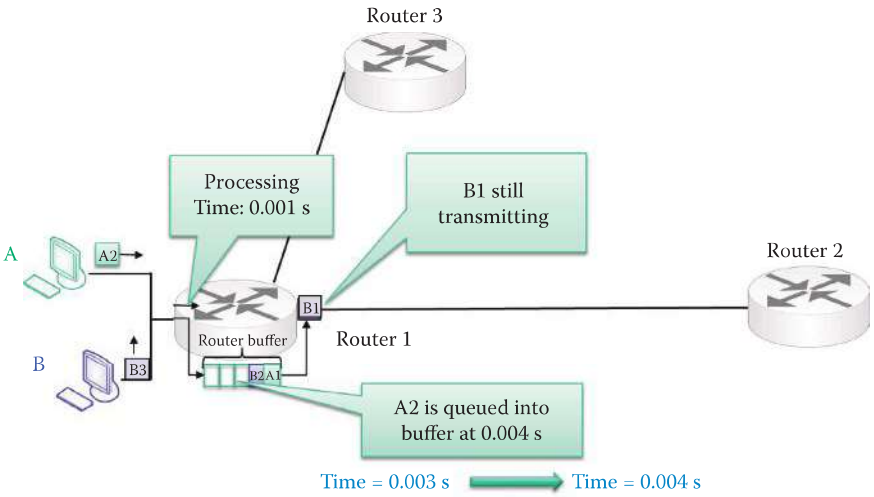


FIGURE I.22 Delay factor example at time 0.003 s.

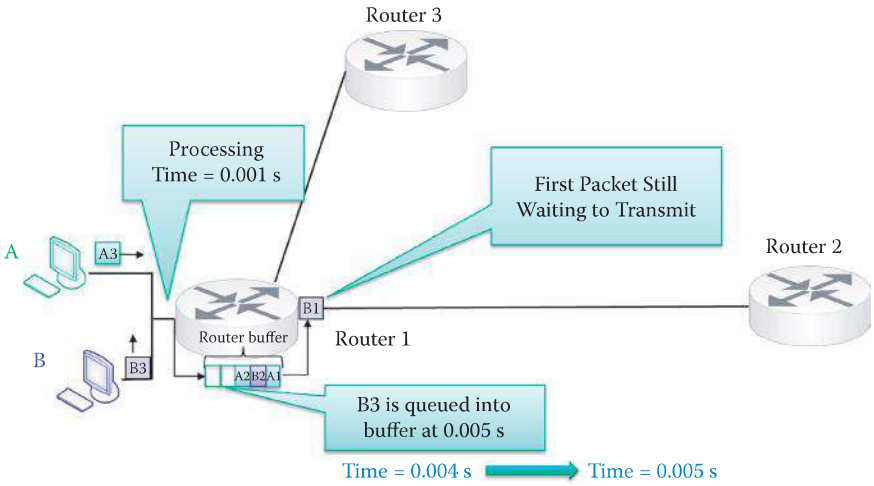


FIGURE I.23 Delay factor example at time 0.004 s.

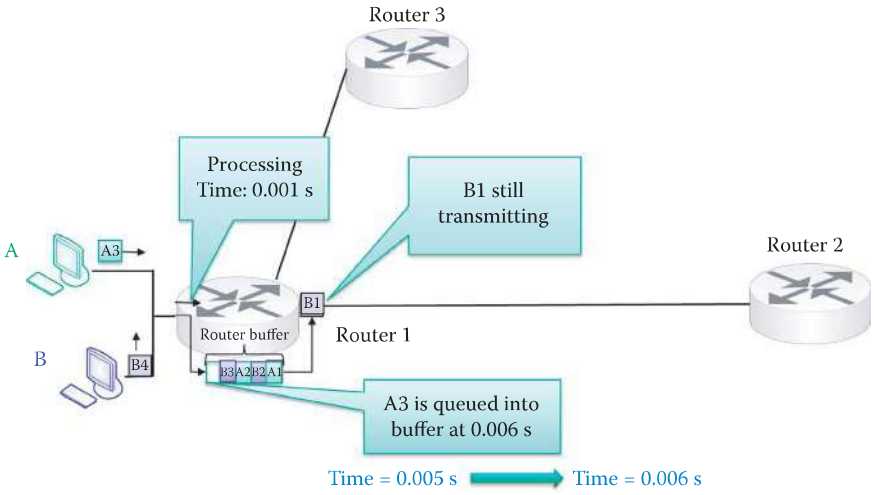


FIGURE I.24 Delay factor example at time 0.005 s.

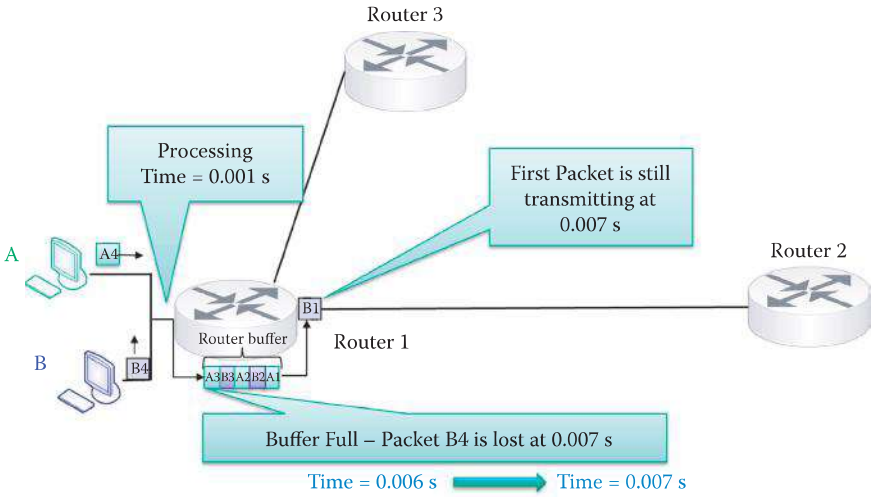


FIGURE I.25 Delay factor example at time 0.006 s.

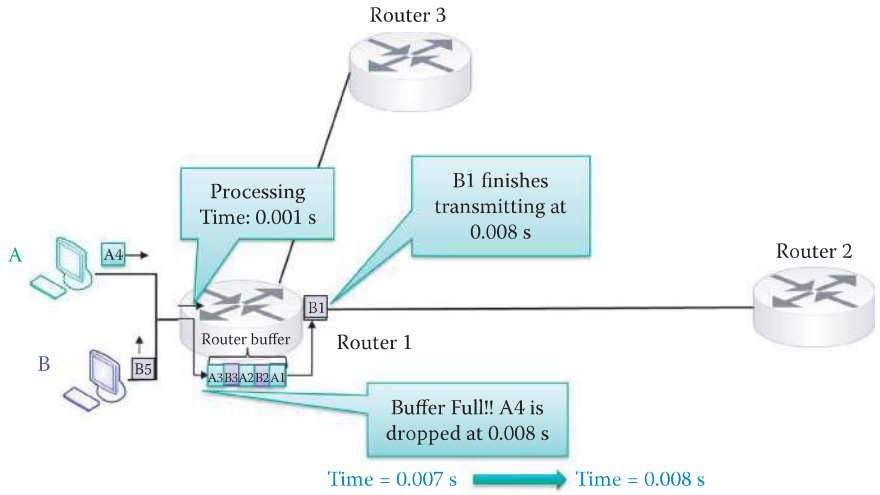


FIGURE I.26 Delay factor example at time 0.007 s.

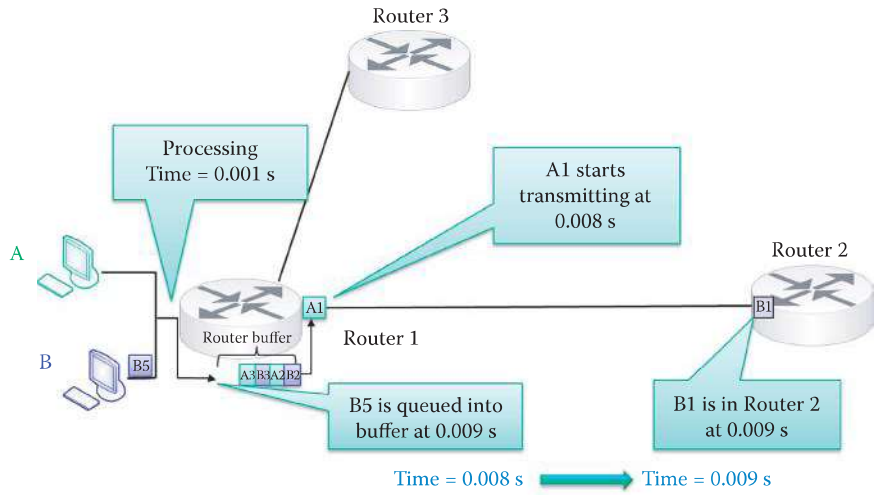


FIGURE I.27 Delay factor example at time 0.008 s.

I.6.3 CONGESTION AND FLOW CONTROL

Congestion is a natural consequence, which results when a source host sends out more data than the network and destination host can digest. This situation is even exacerbated by the fact that destination hosts can range from servers with fast Central Processing Units (CPUs) and high-speed links to smartphones with low-power CPUs and slower links. These situations can result in busy links and router/switch buffer overflow due to finite buffer size.

Given this situation, the obvious question is—how do we cope with this resulting congestion when the bandwidth and buffer size are unable to meet the required demand? When using Transmission Control Protocol (TCP) during congestion, resending packets, resulting from packet delay or loss, causes further loss and delay, and the negative feedback will cause even more congestion. So, the answer is flow and congestion control, which attempts to alleviate this condition by throttling back the output rate of the source host to relieve the congestion. The symptoms of congestion that trigger the congestion control are packet loss and delay, as well as buffer overflow. Flow control is used to tell the source host how much information the destination host can digest. The goal of this process is to optimize the throughput rate (bits/sec) between source and destination without causing congestion.

I.7 THE PROTOCOL STACK

It would certainly appear that the intercommunication among computers would require some standardization that would facilitate their successful interactions. There should be some "protocol" that defines the manner in which they talk to each other so that messages are clearly understood. It is this "protocol", documented in a stack that is accomplished through modularization, development and upgrades that support operations such as web surfing, email and the like.

Prior to addressing the many facets and ramifications of the protocol stack, it is important to note that activities within the Internet can be approached in a modular fashion and this modularization is accomplished through layering. As a result, numerous aspects and technologies that are applicable are being developed by many diverse individuals and groups through a divide-and-conquer strategy. By its very structure it is clear that the stack consists of different layers, each of which performs a special function.

Modularization of the Internet is accomplished through layering. As a result, the Internet is being developed by many people, and institutions through a divide-and-conquer strategy. For example, using modularization, one company can tackle the development, maintenance, and updating of a single module. There is strong interaction between layers in that each layer relies on the services of the layer below and exports services to the layer above. It is the interface between layers that defines the interaction, e.g., implementation details can be hidden and layers can change without affecting other layers.

I.7.1 THE US DOD PROTOCOL STACK

When computers are connected within a network, guidelines must be established that support their interaction. The architecture that defines the network functionality is split into layers that collectively form what is commonly known as a protocol stack. The U.S. Department of Defense (DoD) model for the Internet protocol stack is shown in Figure I.28. The International Standards Organization also developed a separate protocol stack containing two additional layers, and known as the Open Systems Interconnection model, but that model was never completed.

Each layer of the protocol stack may employ several protocols to implement the functionality of that particular layer. In a natural progression up the stack, the physical layer deals with the transmission of bits that are propagating over such media as copper, fiber or radio. The data link layer aggregates the bits, e.g., into a frame, and performs the data transfer between neighboring network elements using as an example, Ethernet or WiFi. The network layer handles the routing of datagrams, in packet form, from source to destination using routing protocols. The transport layer performs the process-to-process communication using segments, i.e., message transfer using for example (a) Transmission Control Protocol (TCP) for reliable transport with overhead, (b) User Datagram Protocol (UDP) for best effort delivery with little overhead, or (3) Stream Control Transmission Protocol (SCTP) for reliable transport based upon the nature of the transaction. Finally, the application layer, containing the message, supports the various network applications, such as transferring files (File Transfer Protocol, FTP), data transfer on the world wide web (HyperText Transfer Protocol, HTTP), or electronic mail (Simple Mail Transfer Protocol, SMTP).

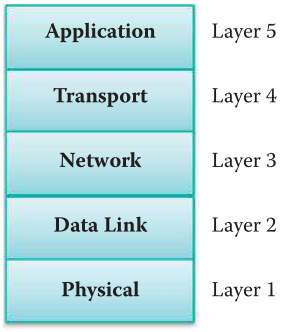


FIGURE I.28 The U.S. DoD model for the Internet protocol stack.

The various applications performed on the network can be typically categorized as either Web-based applications or new protocol/technology development. In the former case, scripts are used for rapid development. For example, JavaScript is employed on the client side and PHP is used on the server side for HTTP applications. There are many other script languages, e.g., Perl, asp, Ruby, and the like. In the latter case, sockets which provide an Application Programming Interface (API) are used by programmers to invoke TCP or UDP. Inter Process Communication (IPC) is extended to the other host in the Internet connection, and information is virtually stored in the device's memory. Socket programming uses Java or C++, and the OS as well as the related firmware/hardware support IPC. The applications invoke protocols for information exchange and, as a result, information is virtually resident in memory with access latency and loss.

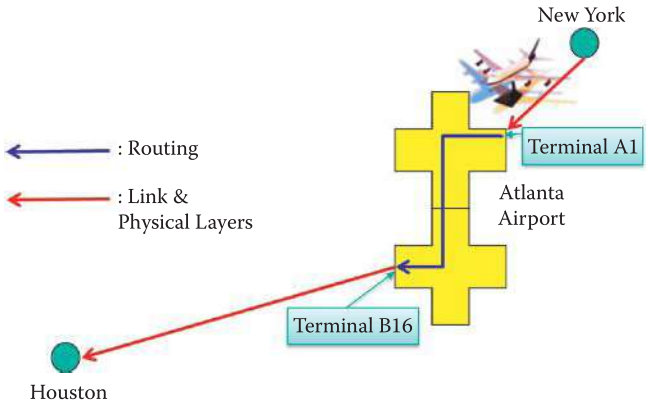


FIGURE I.29 Comparing routing/forwarding with the data link layer.

Example I.5: Network Layer Routing/Forwarding Functions and the Link and Physical Layers

Figure I.29 is used as a vehicle to compare the actions of network layer routing/forwarding with the data link layer. As an analogy, assume someone comes in on a flight and enters terminal A at Gate 1 and must leave on a plane from terminal B, Gate 16. Routing/forwarding from one gate to another would involve moving from one terminal to another terminal using the flight number and monitor guide as aids. The data link is the flight from one airport to another, and the physical layer is invoked by the Link layer.

The Physical Layer defines the means by which bits rather than packets are transmitted over a physical link connecting two network nodes. This bit stream may be grouped into code words or symbols and converted to a physical signal that is conveyed over a transmission medium. The Physical Layer performs character/symbol encoding, transmission, reception and decoding. The transmission media include such things as copper, twisted pairs or coax, fiber and radio. The encoding of the physical layer defines the manner in which each bit/symbol can be represented as voltage, current, phase, frequency, or photons.

I.7.2 THE OSI PROTOCOL STACK

The International Standards Organization (ISO) [24] has developed the protocol stack shown in Figure I.30, referred to as the Open Systems Interconnection (OSI) model. In contrast to the DoD Internet stack, this latter model has seven layers. The two additional layers that lie between the transport and application layers are the session and presentation layers. The session layer aggregates connections for efficiency, synchronization, and recovery in data exchange. The presentation layer permits applications to deal with coding, encryption, compression and the like. If these services are needed in the DoD model, they must be implemented in the application layer. The OSI stack was never completed, but the U.S. DoD had sufficient funding to complete the development of its protocol stack.

FIGURE I.30 The ISO protocol stack.

I.7.3 PACKET HEADERS AND TERMS

Each layer in the stack, with the exception of the physical layer, has a header. These headers facilitate the communication of information and are analogous to an envelope that contains both source and destination addresses. The link layer has a header containing Media Access Control (MAC) addresses, the network layer has a header containing Internet Protocol (IP) addresses and the transport layer has a header containing the port, i.e., service number.

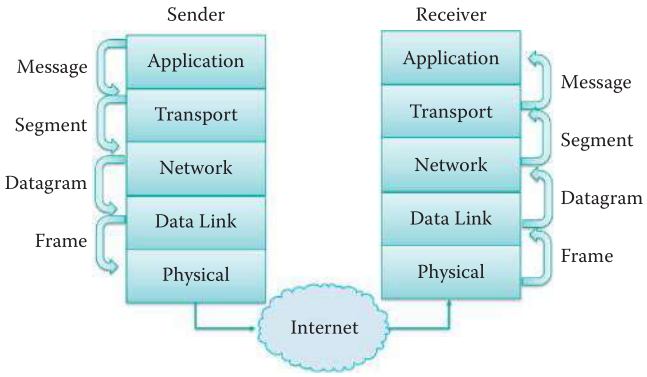


FIGURE I.31 The Internet protocol stack and associated packet identifiers.

The Internet protocol stack and associated packet identifiers are shown in Figure I.31, where the terms *message*, *segment*, *datagram*, and *frame* are used for the following corresponding layers: application, transport, network and data link.

I.7.4 THE LAYER 2 (L2) TO LAYER 5 (L5) OPERATIONS

Given the protocol stack and the manner in which a packet of information progresses through this stack with the attendant headers that are applied at each level, let us now consider in some detail the switching that takes place as the packet moves from layer to layer.

Example I.6: An Overview of Layer 2 to Layer 5 Operations Performed at the Source Host, L2 Switch, L3 Router and Destination Host

The manner in which a message is sent from source to destination over the network is illustrated in the figures that range from Figure I.32 to Figure I.35. As indicated earlier and illustrated in Figure I.32, the protocol stack consists of layers, with one or more protocols supporting each layer. Each protocol may be implemented in a combination of hardware and software.

Suppose now that an application has a message to send to a destination. This message employs application protocols such as HTTP and FTP. The message is passed to the transport layer. For Internet use, the protocols used at this layer are TCP or UDP. At this point, the message is segmented and a transport header is attached to each segment, which contains the port number of the transport layer, i.e., both source and destination port numbers. The port number of a server indicates the application layer protocol, e.g., port 80 for HTTP. The transport layer segments are then passed to the network layer where the destination's IP address is added. At this point, the message has, in essence, a destination IP address and a source IP address. It is the responsibility of the network layer of the source host and involved routers as well as the destination host's network layer to deliver the segments, also known as packets or datagrams, to the transport layer at the destination. The network layer of hosts and routers contains the routing protocols necessary for this delivery. The destination IP address is obtained through DNS from a URL. The network layer passes the datagram on to the link layer. While the network layer routes the packets from source to destination through one or more routers, the link layer only knows how to progress from one interface to the next interface connected by a physical link. The link layer creates a frame containing the datagram, and is responsible for moving this frame to the next adjacent interface in the transmission path. The link layer adds the MAC address of the next interface, e.g., the router interface, and passes it on to the physical layer. The network layer of the source host knows the destination IP address belonging to another subnet and delivers the frame to the router interface (aka. gateway to the Internet). The destination MAC address is obtained using the ARP (Address Resolution Protocol) from the IP address of the

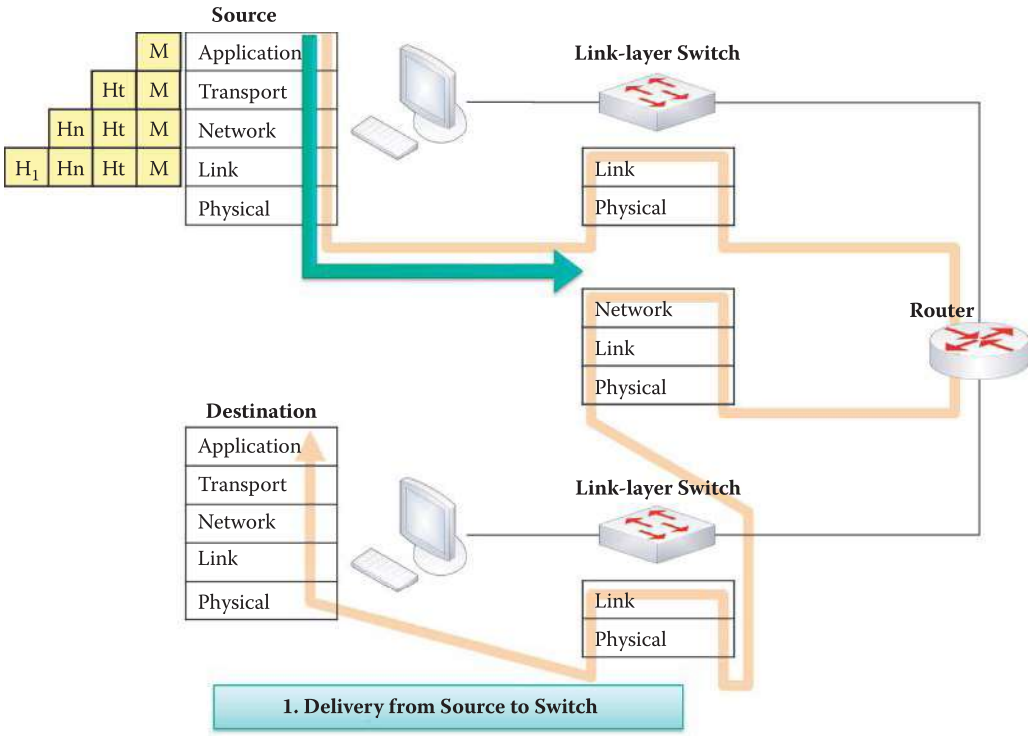


FIGURE I.32 Source to destination illustration—delivery from source to switch: The headers are added at each layer when the message is passed down the protocol stack. H_t is the transport layer header, H_n the network layer header and H_l the link layer header.

router interface. It is this physical layer that moves individual bits in a manner consistent with the actual transmission medium, such as copper wires. Clearly, what is happening is this: as the original message progresses down the stack each layer adds necessary information to the bits from the layer above.

Example I.7: The Operations Involved in Layer 2 Switch Forwarding

The link layer switch, shown in Figure I.33, is a device whose operation is confined to the bottom two layers of the protocol stack. This switch delivers the frame to the correct hardware output port based upon the destination MAC address in the header. The frame is forwarded to the router interface that has the destination MAC address.

Example I.8: The Operation of a Layer 3 Router

While the layer 2 switch's operation is based on the MAC address, the router is a layer 3 device, as indicated in Figure I.34. Thus, the router will route the datagram/packet based on the destination IP address, which has been supplied by the source host. Knowing the destination's IP address, the router must now use the proper destination MAC address for packing the link layer header. Therefore, the new destination MAC address is used by the next link-layer switch in order to forward the frame.

Example I.9: The Link-Layer Switch Functions in Delivering a Frame to the Destination Host

As indicated in Figure I.35, the link-layer switch delivers the frame from the router interface to the correct output port of the switch based on the destination MAC address, which is burned into the incoming interface of the destination host. The frame is then sent to this destination host.

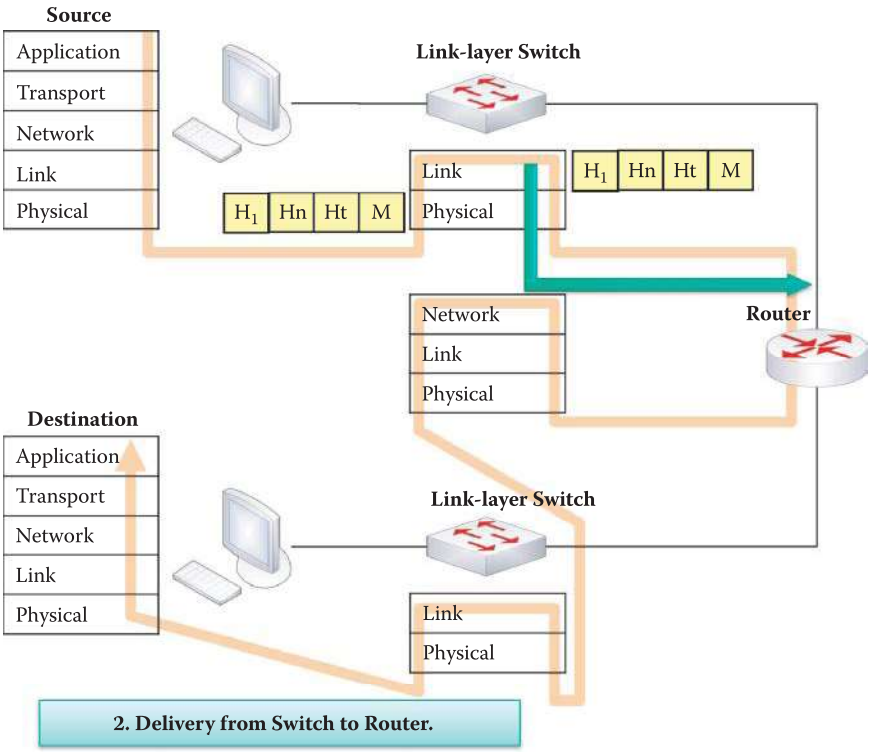


FIGURE I.33 Delivery from switch to router.

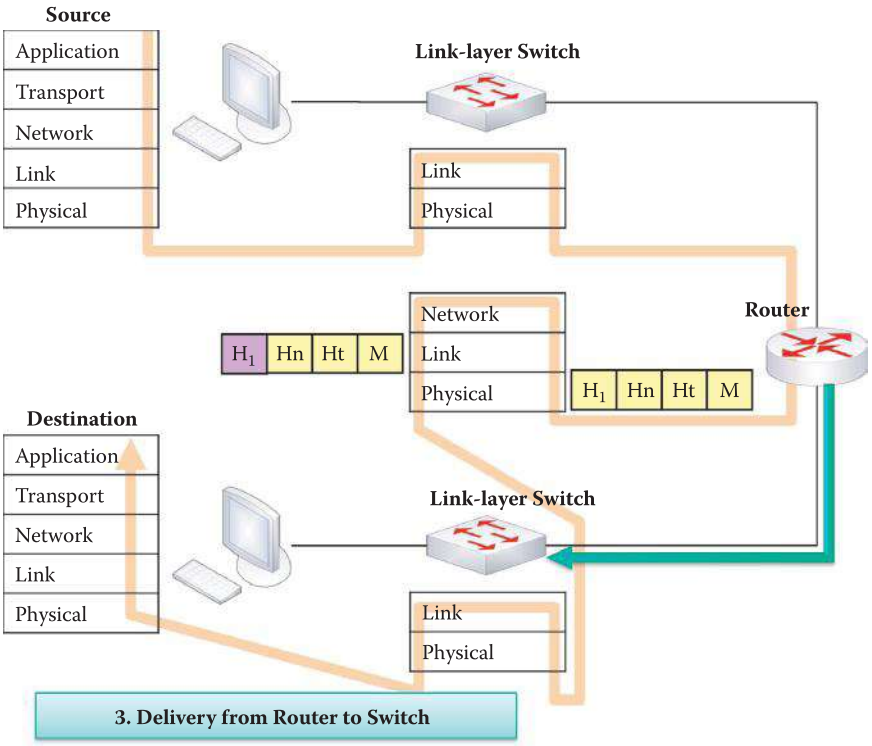


FIGURE I.34 Delivery from router to switch.

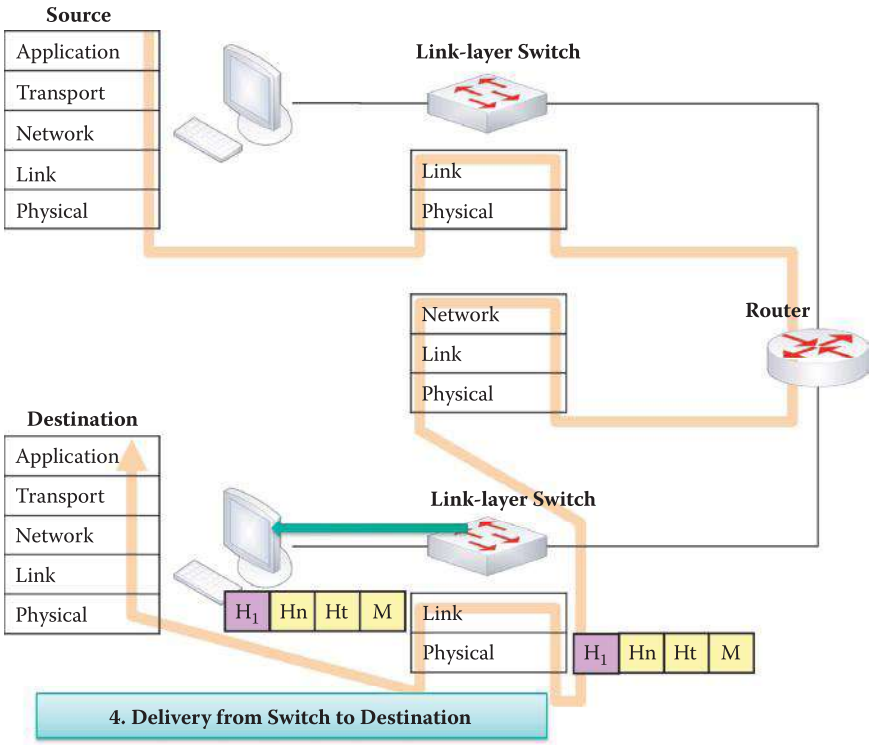


FIGURE I.35 Delivery from switch to destination.

Example I.10: The Operations of the Protocol Stack in Processing Frames at the Destination Host

Upon the frame's arrival at the destination host, as shown in Figure I.36, the frame progresses up the stack. The link layer takes the bits, strips off the header, containing the MAC addresses, and passes the packet/datagram up to the network layer. The network layer strips off the header containing the IP address, and passes the segment to the transport layer. The transport layer strips off its header, assembles the bytes, and passes the information to the proper port for the particular application, e.g., one port in a browser may be for Fox News and another for Amazon, if both ports are in use. Finally, the application layer, working in conjunction with the transport layer, reassembles the segments to form the message that was originally sent.

Example I.11: An Explanation of the Differences among Layer 2 and Layer 3 Operations

Having examined the progression of a message from source to destination through the various network elements, consider now some of the salient features of these elements. For example, the Layer 2 (Link-layer) switch cannot change the destination and source MAC address under any circumstances. However, it does know the port that is associated with the destination MAC address, and thus can process the packet and direct it toward the correct port. The layer 2 switch learns this information from the header that contains the source's MAC address. Thus, this learning process yields a switching table that is used to direct the packet. The source computer has to know the IP address of the first gateway, i.e., router, and employs the Address Resolution Protocol (ARP) to obtain the gateway's MAC address. The destination MAC address of the packet exiting the source host is the MAC address of the first router's interface, while the destination IP address is that of the terminal host.

In contrast to the layer 2 switch, routers and/or layer 3 switches understand both MAC and IP addresses. Routers work in concert with one another to generate routing tables. The routing table provides the router or layer 3 switch with the next hop's IP address. The router

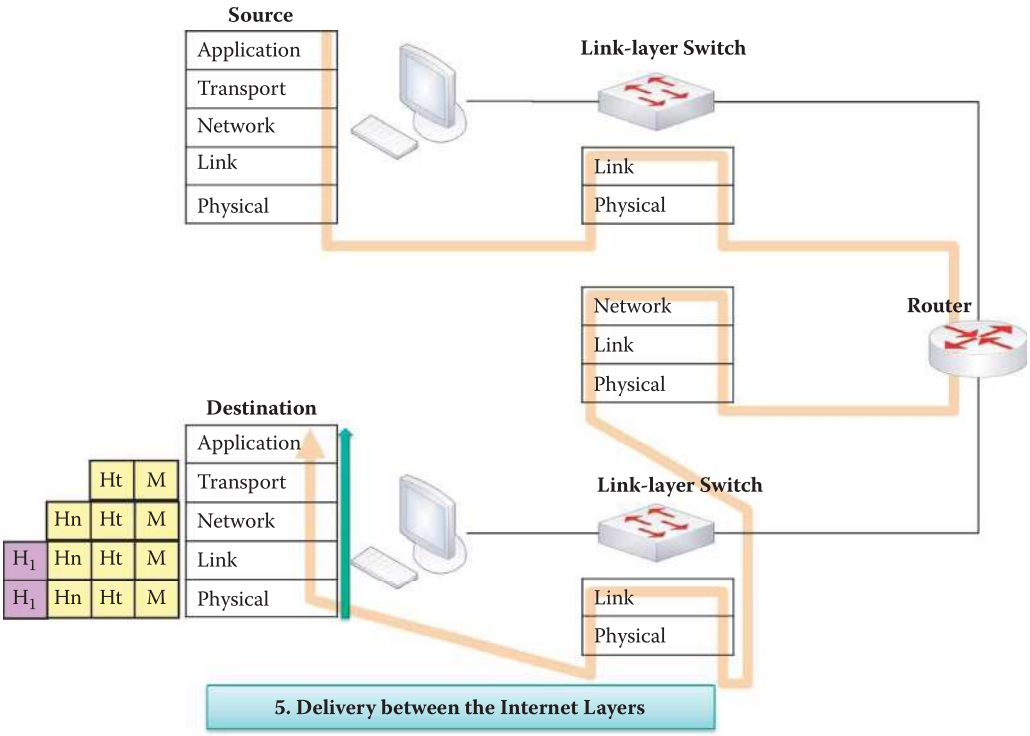


FIGURE I.36 Delivery between Internet layers at the destination host.

then uses the ARP to determine the MAC address of the terminal host. Once this destination MAC address is changed by the router, the layer 2 switch that lies between the router and the next host, can switch correctly. Therefore, the layer 2 switch learns from the source MAC address to derive the switching table, and the routing mechanism is learned from the routing table. The details of this process are found in Part 3 of this book.

I.7.5 A USER'S PERCEPTION OF PROTOCOLS

The manner in which a user employs the various protocols when accessing the web is outlined in the following example.

Example I.12: The Steps Involved in Connecting a Host to the Internet and Downloading a Webpage

The steps involved in using the Internet are outlined in Figure I.37. This figure specifically details the elements involved in the use of HTTP to access a web server. Although we have demonstrated the steps involved in using the Layer 2 and 3 protocols in the figures that began with Figure I.32 and ended with Figure I.36, there are a variety of protocols, and all communication and activities within the Internet are governed by them. For example, the Dynamic Host Configuration Protocol (DHCP) provides a client with an IP address, gateway IP address and DNS IP address. In general, protocols define the packet format, the sequence of packets sent and received among network entities, and the actions that take place based on the parameters contained within the fields of a received packet. The service (port) number is embedded in the TCP header, e.g., port 80 for HTTP. Sequence and acknowledgment numbers are also contained in the TCP header for tracking loss. Retransmission of a packet depends on the acknowledgment number obtained from the receiver. Clearly, it is important for all devices to use and understand the same language. That is why this *language* is specified as a standard that is set by the IETF, because syntax and semantics are critical in this environment.

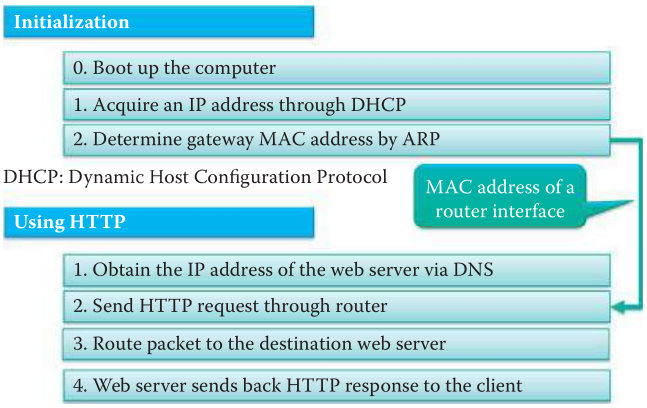


FIGURE I.37 The procedural steps for using the Internet.

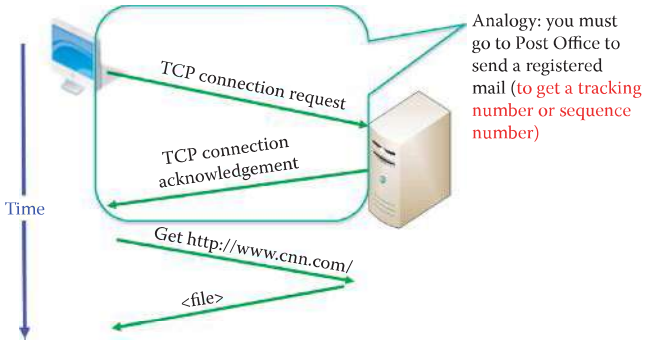


FIGURE I.38 The operation of the HTTP protocol.

As shown in Figure I.38, the HTTP protocol establishes a connection between client and server so that reliable delivery of information, e.g., the use of a packet sequence number for loss detection, can be established for the socket. Connection-oriented service derives its name from the establishment of a connection for reliable transport. The round-trip connection establishes parameters such as a sequence number and round-trip time (RTT) so that the sender will be able to retransmit a lost packet if no acknowledgment is received. In this HTTP protocol, the client makes a TCP connection request, the server sends back an acknowledgment, the client then requests the required data, which is then supplied by the server.

I.7.6 A COMPARISON OF THE CONNECTION-ORIENTED AND CONNECTIONLESS APPROACHES

Example I.13: The Overhead Involved in the Connection Oriented Approach (TCP) for Sending a File from a Host to the Server in Figure I.38

In using a connection-oriented approach, TCP requires a round trip for establishing a TCP connection prior to delivering a file. Suppose the file to be delivered is 4000 bytes in length and uses a link that has a 1.536 Mbps bandwidth and a 1ms propagation delay. Let us consider the percent overhead required to establish this connection and send the file from host A to host B. Neglecting other delays,

The overhead = indirect cost/total cost.

The total delay = round trip delay incurred in establishing a TCP connection + delay in sending the file = 2* 1 ms + 4000 * 8/(1536000) + 1 ms = 2 + 20.83 ms + 1 ms = 23.83 ms

Thus, the overhead = 2* 1 ms/23.83 ms = 8.39%.

Example I.14: The Overhead Involved in the Connectionless Approach (UDP) for Sending a File from a Host to the Server

In using a connectionless approach, UDP does not require a round trip for establishing a TCP connection before delivering a file of 4000 bytes using a link that has a 1.536 Mbps bandwidth and a 1 ms propagation delay. Hence, there is no overhead associated with UDP.

Protocols, such as Ethernet 802.3 [6], IP, TCP and HTTP, perform a number of very important functions. For example, they govern the movement of packets from source to destination under the specifications of certain standards, take actions that are specified in the packets, manage packet flow and congestion for optimal performance and even recover lost packets, which require a connection oriented transport protocol (TCP). The protocols work in conjunction with one another to accomplish the specified task requested by the user. Applications, such as HTTP, invoke transport protocols, such as TCP; transport protocols invoke the IP protocol; and the IP protocol invokes Ethernet or something similar. In support of all of these functions are the Domain Name System (DNS) and other protocols, such as the Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP) and Internet Control Message Protocol (ICMP) that provide the glue that holds everything together. DNS and DHCP typically employ UDP since the information transmitted is very small and the connectionless approach (UDP) reduces overhead.

With the use of these protocols, the Internet becomes a distributed information sharing and delivery service. As such, the Internet supports distributed applications and services, such as a data sharing service involving the Web, email, games, e-commerce and file sharing, as well as a real-time service for the delivery of VoIP, video conferencing and IP TV. The transport services provided to applications are either a reliable data delivery service from source to destination that is characterized by more overhead, no tolerance for error or loss, but capable of tolerating delay and jitter, i.e., TCP, or a best effort, but unreliable, data delivery service that has less overhead, able to tolerate error and loss, but unable to tolerate jitter, i.e., UDP. The former transport service is good for data, such as email, and the latter transport service is good for voice and video.

I.8 PROVIDING THE BENEFITS OF CIRCUIT SWITCHING TO PACKET SWITCHING

In our earlier comparison of circuit switching and packet switching, it was indicated that while packet switching possessed a number of important and advantageous features, it was generally not suitable for voice and video. However, because it is useful in so many ways, we are naturally led to ask the question—isn't there some method that can be employed to make the packet switching-based Internet suitable for delivering voice and video?

When packet switching is employed, the data stream for each host is segmented into packets, and the destination IP address is contained in the packet header in the same way in which a standard letter would have the address written on the envelope. Each packet travels independently using the available resources provided by the routers. Packets may be lost or arrive out of order. It is the job of the transport layer at the destination to reassemble the received packets in the correct order.

In the real world there are typically finite resources, and all hosts must share them. For example there is only so much link bandwidth and router/switch buffer space. However, each packet uses the full link bandwidth during transmission and thus must compete for resources with other packets. Available resources are typically used on an as-needed basis. When the aggregated resource demand exceeds the amount available, congestion occurs. Packets are then placed in a queue and wait for the next available link, just as vehicles would do when a traffic jam turns a busy highway into a parking lot. Unlike the traffic analogy however, queue overflow can occur if packets overrun the available space in a router/switch and in this situation the excessive packets are dropped.

In order to maintain some Quality of Service (QoS), resource allocation and reservation is necessary. This is critical for voice and video and is typically organized so that all resources are fully utilized. Performance is optimized by strategically dividing resources among the competing

parties. These resources are link bandwidth, packet priorities in router and switch queues, the memory/buffer/queue in routers and any wireless spectrum needed.

Because both packet switching and circuit switching possess some distinct advantages, an obvious issue is the combination of the two. There are two approaches to this combination. The Telco approach employs ATM. In this case, a virtual circuit uses a sequence of 53-byte packets called cells that mimic the circuit-like connection, which involves connection setup and teardown. The IP approach uses the Resource Reservation Protocol (RSVP). The RSVP is a Transport Layer protocol for reserving resources in order to achieve an integrated services Internet. The approach that is IP-based uses protocols based on IP for streaming video/audio over the Internet. These protocols are the Real-time Streaming Protocol (RTSP), the Real-time Transport Protocol (RTP) and the Real-time Transport Control Protocol (RTCP). RTSP permits the reservation of resources for a flow using RSVP and relies on RTP and RTCP for delivering audio/video datagrams. RTCP is used by RTP to ensure the QoS. An IP Multicast provides a means to send a single media stream to a group of recipients on the Internet. In contrast, Unicast sends one copy to each recipient causing excessive and unnecessary backbone traffic.

I.9 CYBERSECURITY

Although the targets for cyber attacks may vary widely, they are primarily focused on money, intellectual property and, of course, sabotage. Cybersecurity is a collection of defensive technologies (hardware/software), processes and practices designed to protect networks, computers, programs and information from attack, damage or unauthorized access in order to secure systems that are connected to the Internet. By definition, Cybersecurity protects against threats using defensive measures, including information assurance, computer systems, and applications hardening, malware protection, access control, information infrastructure protection, and network security.

I.9.1 ATTACKS AND MALWARE

Attacks on the Internet information infrastructure originate from the four corners of the world and can be absolutely devastating. The attacks on hosts are generated through malware and can easily gain unauthorized access to critical information. Another form of attack is the denial of service (DoS) attack in which legitimate users are denied access to resources. These DoS attacks will typically exhaust the server's memory and processing capacity and/or exhaust the link bandwidth. Imagine for a moment the impact of overwhelming the communications to a police headquarters in a large city.

Malware comes in five distinct categories/capabilities: (1) *Spyware*, (2) *Viruses*, (3) *Worms* (4) *Trojans* and (5) *Rootkits*. Spyware records keystrokes and other crucial activities and uploads this information to a collection site. A virus provides illegal access to a host's resources, infects it, e.g., through an email attachment, and may contain spyware, Trojans or worms. It is also capable of propagating to other hosts. A host can be infected through a worm by simply passively receiving an object that executes itself and then actively propagates to other hosts. Trojans that may be contained in spyware, a virus or a worm provide a backdoor for illegal access to a host. Rootkits are malware that is hidden in a host's file system and very difficult to detect. Currently, a single piece of malware may possess these 5 types of malware in order to expand its territory, control the infected hosts and steal information.

I.9.1.1 THE ZERO-DAY ATTACK AND MUTATION IN DELIVERY

The usefulness and importance of the Internet could hardly be overstated. However, these qualities are dependent upon the assurance that the information flow from source to destination is secure. And yet, we regularly hear stories that in fact the Internet is vulnerable to a variety of attacks, many of which can have devastating consequences. We are thus first led to ask "why is the Internet so vulnerable?" and "can we detect the malware as an initial step in reducing its effects?"

In addressing these questions we find that security improvements for hosts and the Internet must be approached at every juncture. Security must be incorporated at all protocol levels, the host Operating System (OS) must be hardened, and anti-malware capability must be installed in all hosts and routers. While it is believed that the host operating systems and the numerous applications present the weakest link in the Internet from a security standpoint, the vulnerabilities extend to router and switch firmware, firewalls and protocols. It is most unsettling to find that the security company, F-Secure, believes that the quantity of malware produced in 2007 was equivalent to that produced in the previous 20 years. To make matters worse, some of the malware mutates, i.e., changes form all by itself as it moves from one host to another. In addition, the zero-day attack, i.e., one that is brand new and has no signature, can be non-detectable, and therefore lethal. One must be aware that the life-cycle time of a piece of malware was reduced to two hours in 2009 [18] and this fact indicates that signature-based detection methods were no defense.

Malware is delivered in a variety of ways. It may be carried in an email or in the form of a worm that will self-propagate through the network. Websites are perhaps the worst sources of malware. The following list outlines some of the reasons that malware is such an enormous problem: it can mutate during propagation in a varying formation in order to defeat malware detectors; it can hide in a PC's BIOS where it cannot be detected; it can rewrite the first block of the hard disk or solid state drive so that detectors cannot be initialized; and it can upgrade itself to defeat or disable the newest defense measures delivered by software updates.

I.9.1.2 CRIMEWARE TOOLKITS AND TROJANS

Given the level of trouble that can be created with malware, it is reasonable to ask just how much crimeware actually exists? The answer is much too much. Why is there so much? The answer to this question is simply that it is cheap to get in and the business is very lucrative for profits or intellectual property. As a result, there are numerous versions of malware that are available for purchase. For example, the security firm, McAfee, has published an analysis of the "Zeus Crimeware Toolkit" [19]. An individual can purchase Zeus ($4000/copy) or the SpyEye crimeware toolkit (for about $500) [20]. For example, the ZeuS Trojan toolkit version, which is an attacker's package, allows criminals to make a customized web site in just a few clicks, and lure unsuspecting people to it. Then, their machines are infected with the malware, which may propagate to other hosts. Botnets (Zombies) can be established by an attacker for command and control or can be rented for profit. Symantec alone has detected that over 154,000 computers are infected with the Zeus Trojan and there existed 70,330 unique variants of the Zeus Trojan binary in 2009. Global tracking of ZeuS Command and Control servers (hosts) is performed by the ZeuS Tracker at https://zeustracker.abuse.ch/, while SpyEye Command and Control servers are globally tracked by the SpyEyeTracker at https://spyeyetracker.abuse.ch/. The totality of malware presents a clear danger for the legitimate user.

The ZeuS Trojan has the capability to capture passwords, even a one-time password. The security experts found that ZeuS is able to read PINs and transaction numbers (TANs) entered not only via keyboards, but also via mouse clicks [21]. RSA Security provided a service to verify a transaction using SMS in order to protect a one-time password against Zeus. According to a report on the S21sec blog, new versions of the ZeuS banking Trojan are now homing in on the SMS-TAN procedure, also known as mobile TAN or mTAN. In the SMS-TAN procedure, transaction numbers (TANs) for online transactions are sent to the customer's cell phone to authenticate that person for an online bank transfer that has been initiated, for instance, from a web browser. The use of the second communication channel for confirming the transaction is designed to make phishing and Trojan attacks impossible. After all, the transaction can only be hacked if users do not carefully check the data in the text message, if their cell phones get stolen, or the device is infected with a Trojan that passes on the text message to the phisher.

However, the developers of ZeuS have pursued the last strategy to get Trojans onto mobile devices for an attack requiring multiple stages. The most important step is still infecting a Windows PC. In this case, victims view a specially crafted web site that masquerades as a security update for the victim's cell phone. Victims are asked to enter their cell phone number so they can receive a link for the download in a text message. The PC infected with the Trojan then promptly sends a text message containing a link to what appears to be a new security certificate. Users

are then asked to download and install the certificate on their mobile phones, which requires an Internet connection on the phone. The downloaded file contains the mobile version of ZeuS, which then analyzes and forwards all incoming text messages. It also executes commands sent via SMS. S21sec says there is a version of the Trojan for Symbian (.sis) and BlackBerry (.jad). Criminals can then use the account access data stolen from the PC along with the TAN to make bank transactions from the account. On 10/19/2011, a variant of SpyEye was found to have the ability to infect a computer, steal the victim's logon credentials and change the phone number that the bank uses to confirm transactions [22].

Police in the U.K. have arrested 19 people on charges they used the Zeus Trojan to steal more than $9.4 million from U.K. banks in September 2010. The bank software tracked the malware activity in the bank customers' computers and identified the attackers. With better security training, those hackers would have cleaned their trails in those computers, which would have made it harder for the police to trace them.

I.9.1.3 SOPHISTICATED MALWARE

Given the plethora of malware that exists and appears to be in a constant state of development, one is naturally led to ask the question: is it possible to escape an attack? Unfortunately, the answer to this question is no if you are being directly targeted by an entity that possesses the proper expertise and resources. A family of recently developed sophisticated malware is listed in Table I.3, and all shared a basic toolkit for malware development.

History would indicate that one of the world's most sophisticated malware is the Stuxnet worm [23] that is designed to attack the Siemens SimaticWinCC supervisory control and data acquisition (SCADA) system. These SCADA systems are installed in big facilities, like nuclear plants and utility companies, to manage operations. Step 7 is the Siemens software used to program and configure the German company's industrial control system hardware. Stuxnet works by infecting Windows machines using four zero-day vulnerabilities. One is used to spread the worm to a machine via a USB stick since the SCADA systems are isolated from the Internet. The second is a Windows printer-spooler vulnerability used to propagate the malware from one infected machine to others on the network. The remaining two help the malware gain administrative privileges on infected machines to feed the system commands. Furthermore, the Step 7 propagation vector would insure that already-cleaned PCs would be re-infected if they later opened a malicious Step 7 project folder. Stuxnet searches for a way to reach the SCADA's programmable logic controller (PLC) and then takes control of the PLC and potentially alters the commands it sends through to the nuclear plants. It is capable of bypassing any other computers that are not Siemens SimaticWinCC machines. It is specifically designed for sabotage and reaches a level of sophistication that has not been seen before. The malware is digitally signed with legitimate certificates stolen from two certificate authorities in order to fake authenticity.

Flame is another unprecedented, sophisticated malware that relies on fake Microsoft certificates for Windows Update to infect fully patched Windows computers in addition to using zero-day attacks. Flame in an infiltrated computer acts as the man in the middle, intercepts a Windows Update request from a victim and infects it by installing bogus Windows Update software. The most detrimental capability of Flame is the feature it employs to forge certificates signed by Microsoft [24]. After infecting a Windows computer, Flame manipulates its microphones, cameras, and Bluetooth to collect intelligence in the immediate vicinity. The defense against this kind of innovative, advanced malware is not available yet and can only be patched once the malware is discovered.

TABLE I.3 A Cyber Espionage Malware Family's Main Features

Malware	Date of operation	Size	Special features
Stuxnet	June 2009	500 kilobytes	Sabotage program: sabotaging uranium centrifuges
DuQu	September 2011	300 kilobytes	Information gathering
Flame	March 2010	20 megabytes	A spyware program; Windows Update deception; Connect with Bluetooth devices in the area

I.9.2 DEFENSIVE MEASURES FOR CYBERSECURITY

Let us now consider the mechanisms that an enterprise can employ to defend itself against malware that is expanding in both scope and sophistication. In order to be active in the business community and use the Internet, defensive measures simply have to be used. Table I.4 lists the typical security devices/software, widely deployed by enterprises and described in the following sections.

I.9.2.1 THE FIREWALL, THE INTRUSION DETECTION SYSTEM (IDS) AND THE INTRUSION PREVENTION SYSTEM (IPS)

While it would appear that this malware is capable of destroying the Internet and everyone attached to it, the industry is not standing idly by watching everything this ubiquitous communication system has provided made useless. A tremendous industry has been established worldwide to address these problems. Three of the methods that are employed to protect systems are the *Firewall* [25], the *Intrusion Detection System (IDS)* and the *Intrusion Prevention System (IPS)* [26]. These elements are typically placed at critical entry and exit points to protect vital assets, such as a server farm, a financial database, or something else of significant value.

Host firewalls are used in a computer's OS/application to protect the host. Network firewalls are used to protect the entrance to a network and block packets based on the IP address and port number in the header (L3 to L4). In addition, a stateful inspection is performed in order to maintain a state transition table for a connection. Both IDS and IPS are used to monitor potentially malicious traffic by inspecting the entire packet (L2 to L5). IDS will let the packet pass, but sends an alert to the network administrator, while IPS will block a malicious packet and send a message to the network administrator.

A firewall operates in the manner shown in Figure I.39. Its purpose is to isolate an organization's internal network. As the arrows in the figure indicate, the firewall permits transmission from the organization to either the public Internet or the *Demilitarized Zone (DMZ)*, as well as transmission from the DMZ to the Internet. However, it blocks traffic into the organization from either the public Internet or the DMZ.

TABLE I.4 An Overview of Typical Security Devices/Software

Name	Security check	Action taken
Firewall	TCP/IP packet header inspection	Block
Intrusion Detection System (IDS)	TCP/IP packet header and content inspection	Alert
Intrusion Prevention System (IPS)	TCP/IP packet header and content inspection	Block and alert
VPN: SSL/TLS	Authentication, encryption and integrity	Communication protection
VPN: IPsec	Authentication, encryption and integrity	Communication protection
Network access control (NAC)	Host health inspection, authentication, encryption and integrity	Access control

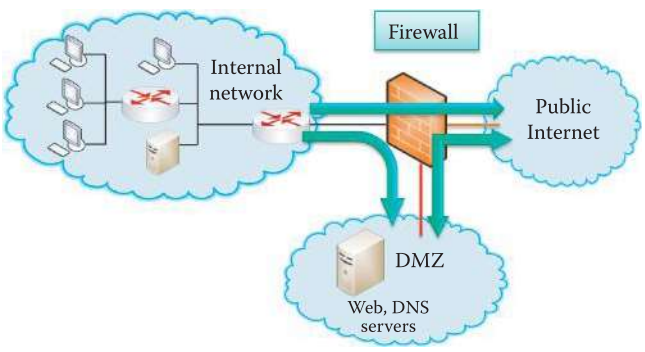


FIGURE I.39 Firewall protection for an organization.

As shown in Figure I.40, IDS/IPS is strategically placed at the entrance to an organization. From this vantage point it can detect a wide range of attacks. Attackers typically perform network mapping, in the form of reconnaissance using nmap, as well as port scans and TCP stack scans that can be detected/blocked by the IDS/IPS. It can also detect denial of service bandwidth-flooding attacks, worms and viruses, as well as both OS and application vulnerability attacks. The IDS/IPS can also be provided by software in a computer, which is usually integrated with anti-virus software. One must be cognizant of the fact that signature-based detection methods used in IDS/IPS and anti-virus software are ineffective against any zero-day or mutated malware. The IDS generates too many false positive alarms, which make it difficult for administrators to identify meaningful attacks. On the other end, the IPS only blocks the packets that are definitely malicious while other malicious packets pass through. It is the responsibility of every user to take precautionary measures, by employing the help of currently available defense products, when surfing the Internet.

Today's fully featured routers contain within them the firewall and IDS/IPS functions, which can be configured to perform the specified functions. It is for this reason that modern vendors typically claim that their routers perform the L2 to L7 switching functions.

I.9.2.2 VIRTUAL PRIVATE NETWORKS (VPN) AND ACCESS CONTROL

While it is clear that defensive measures must be applied at every possible location, the communication, which often carries sensitive information, must also be protected. There are several methods that can be employed with information transmission. Chief among them are *encryption*, *authentication* (credentials that state you are who you say you are coupled with integrity protection) and *authorization* (which verifies that you have permission to access the specific resources). For example, Secure Socket Layer/Transport Layer Security (SSL/TLS) [27] is used between the session and transport layers for such things as Internet shopping and web mail. The Internet Protocol Security (IPsec) [28] is used in the network layer for such things as a virtual private network (VPN), as shown in Figure I.41, and VPN is allowed to pass through a corporate firewall.

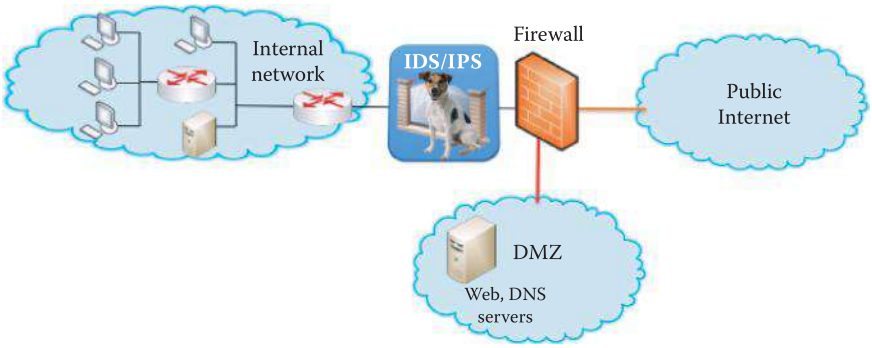


FIGURE I.40 Placement of the IDS/IPS protection system.

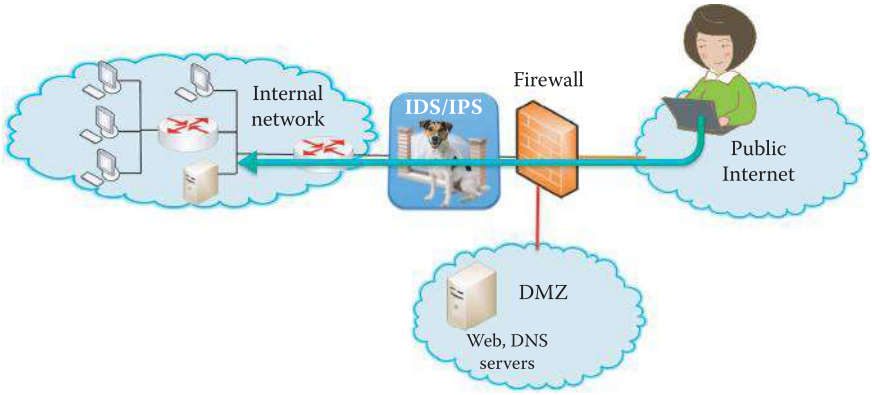


FIGURE I.41 A user can use VPN tunnel to securely pass through a firewall from the public Internet.

Organizational network access control (NAC) is agent-based NAC deployed at each host and central control server. Only healthy hosts that are certified by their agents can have network access, and security policy enforcement is a main feature of NAC in an enterprise network. 802.11i [8] is used in the data link layer for WiFi or 802.11 WLAN; organizational access control using Active Directory based on Kerberos is used for user access control, RADIUS/AAA protocol is employed for authentication and 802.1x [29] is placed in layer 2 for WiFi and LAN authentication.

Today's routers, including those used in the home, have IPsec or SSL/TLS VPN functions built right into the unit. Therefore, one can simply configure the router to perform the functions desired. The details involved in configuring VPNs will be discussed in Part 5 of this book.

I.9.2.3 INTEGRATED DEFENSE FOR AN ENTERPRISE NETWORK

The integrated defense for an enterprise network has the following formula:

Integrated defense = endpoint security software + cloud + NAC + IDS/IPS + Firewall

Endpoint security software contains an array of layered protection including

- Malware signatures
- Real-time code emulation
- Advanced heuristics
- A cloud-centric feedback loop from actual users, such as reputation services that blocks bad IP addresses, URLs, and files
- Application controls that are effective in decreasing the endpoint attack surface
- Tools provide kernel level, hypervisor level, or CPU level protection to protect against rootkits

The NAC uses centralized policy enforcement for endpoint security, that can be configured in accordance with the role of the user and associated devices and employed by the user for authorizing access. This is the most widely deployed integrated defense strategy in enterprise networks.

I.10 HISTORY OF THE INTERNET

I.10.1 THE DEVELOPMENT OF THE INTERNET

It is interesting to recount the development of the Internet. For almost five decades this ubiquitous information system has impacted, in a significant way, the lives of most people throughout the world. Its development is outlined in chronological order in Table I.5.

I.10.2 THE GLOBAL INFORMATION GRID (GIG) OF THE US DEPARTMENT OF DEFENSE (DOD)

The Global Information Grid (GIG) is a communications project of the United States Department of Defense. It is a secure, robust, optical terrestrial network that delivered very high-speed classified and unclassified Internet Protocol (IP) services to 87 key operating sites worldwide in 2005. Every site has an OC-192 (10 Gbps) pipe. The project is a physical manifestation of network-centric warfare (NCW). Because a robustly networked force improves information sharing, the quality of information and shared situational awareness is enhanced. This shared situational awareness enables collaboration and self-synchronization, enhances sustainability and speed of command, and in turn, has a dramatic effect on mission effectiveness [32].

This project provided nine functional GIG Enterprise Services (ES), i.e., core services, in 2004 and they are listed in Table I.6.

GIG also provides authorized users with

- A seamless, secure, and interconnected information environment
- Real-time and near real-time response of ES

TABLE I.5 The Important Developments in the History of the Internet

Year	Development
1961	Leonard Kleinrock (aka the Grandfather of the Internet) demonstrates the effectiveness of packet switching using queuing theory
1964	Packet switching is employed in military nets
1967	The Advanced Research Projects Agency conceives the ARPAnet
1969	The first ARPAnet node becomes operational. The four initial nodes are at UCLA, SRC, UCSB and UUtah
1970	The ALOHAnet, which is a satellite network, is developed in Hawaii
1972	The ARPAnet is demonstrated to the public and grows to 15 nodes. The Network Control Protocol (NCP) becomes the first host-host protocol, and the first email program is developed
1974	Vinton Cerf (aka the father of the Internet) and Robert Kahn's architecture for interconnecting networks becomes the foundation for the Internet Protocol. Its properties are minimalism, autonomy, best effort service, stateless routers and decentralized control
1976	Ethernet is developed at Xerox PARC, Intel and DEC
1977/78	Proprietary architectures, such as DECnet, SNA and XNA are developed, and ATM is developed for switching fixed length packets in hardware for virtual circuits
1979	ARPAnet grows to 200 nodes
1982	The email protocol, SMTP, is defined
1983	TCP/IP is deployed, and DNS is developed for name-to-IP address translation
1985	FTP protocol is defined
1988	TCP congestion control is developed, and new national networks, e.g., BITnet and NSFnet are developed, and 100,000 hosts are connected to form a confederation of networks
1991	NSF lifts restrictions on commercial use of NSFnet, and network access points are established to connect ISPs
Early 90's	ARPAnet is decommissioned, and the Web comes on-line with hypertext, HTML, HTTP, Mosaic and later Netscape
Late 90's, early 2000's	This period saw the development of the Web, instant messaging and P2P file sharing for music. Network security moved to the forefront. There were an estimated 50 million hosts and more than 100 million users. The backbone links were running at Gbps speeds and field tests of the Internet demonstrated decentralized control. One significant example of the Internet's value was the purchase order from Iraq to a company in Atlanta via email during the first Gulf war when the communication infrastructure was wiped out.
2008 - present	Approximately 1.7 billion users as of September 2009 [30]. The International Telecommunications Union (ITU) estimated two billion users by the end of 2010, and that is nearly a third of the world's total population currently estimated at about 6.9 billion [31]. Voice and video are delivered over IP. The P2P applications in use were BitTorrent (file sharing), Skype (VoIP), and PPLive (video). The social applications resulting from the Internet's development were huge and fostered such things as YouTube, Facebook, Twitter, various types of gaming and web 2.0. In addition, its implications on wireless and mobility proved to be enormous.

TABLE I.6 The Core Services Labeled as GIG Enterprise Services (ES)

Type	
Information sharing	Storage
Communication	Messaging
	Collaboration
Service	Discovery
	Mediation
	User assistant
	Application hosting
Security	Information assurance
Management	Enterprise service management

The GIG must permit both human users of the GIG, as well as automated services acting on behalf of GIG users, to access information and services from anywhere, based on need and capability. Information must be labeled and also cataloged using metadata, allowing users to search and retrieve the information required in order to provide them with the capability to fulfill their mission under a *smart-pull* and information management model. This requires the GIG to know where the information is posted and to recognize the user, regardless of location. While system access will be available regardless of location, access to information will be restricted based on the threat inherent at that location. An enforcement policy must be used to provide user privileges and access to the information, in addition to providing mechanisms, which ensure that the information can be trusted as coming from its claimed source. Thus, security is an embedded feature, designed into every system within the family of systems that comprise the GIG. All the policies are designed to ensure that an adversary is denied the capabilities inherent in the system for bona fide users.

I.11 CONCLUDING REMARKS

In summary, the key concepts that have been presented in this chapter are (a) the Internet architecture comprising the network edge, network core, and access networks, (b) Internet protocol layers and models, (c) the features and differences between packet-switching and circuit-switching, (d) packet loss, delay, congestion and throughput in packet-switching network, (e) the Layer 2 switch, layer 3 switch and router functions, and finally (f) security.

REFERENCES

1. "Internet Engineering Task Force"; http://www.ietf.org/rfc.html.
2. "ICANN - Internet Corporation for Assigned Names and Numbers"; http://www.icann.org/.
3. J. Bingham and F. Van der Putten, *ANSI T1. 413 Issue 2: Network and Customer Installation Interfaces-Asymmetric Digital Subscriber Line (ADSL) Metallic Interface*, 1998.
4. "DOCSIS Specifications"; http://www.cablelabs.com/cablemodem/specifications/index.html.
5. ITU-T Rec., *G.984.1: Gigabit-capable passive optical networks (GPON): General characteristics*; http://www.itu.int/rec/T-REC-G.984.1/en.
6. *IEEE Std. 802.3-2008 IEEE Standard for Information technology-Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CMSA/CD) Access Method and Physical Layer Specifications*, 2008; http://standards.ieee.org/getieee802/portfolio.html.
7. *IEEE P1901: Draft Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications*, 2010; http://grouper.ieee.org/groups/1901/.
8. *IEEE Std. 802.11-2007 IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2007; http://standards.ieee.org/getieee802/portfolio.html.
9. *IEEE Std. 802.11n-2009 IEEE Standard for Information Technology— Telecommunications and Information Exchange Between Systems— Local and Metropolitan Area Networks— Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput*, 2009; http://standards.ieee.org/getieee802/portfolio.html.
10. *IEEE Std. 802.16-2009 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems*, 2009; http://standards.ieee.org/getieee802/portfolio.html.
11. *3GPP specification: 25.306 V5.15.0 (2009-03) 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UE Radio Access capabilities (Release 5)*; http://www.3gpp.org/ftp/Specs/html-info/25306.htm.
12. *3GPP specification: 25.306 V7.10.0 (2009-09) 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UE Radio Access capabilities (Release 7)*; http://www.3gpp.org/ftp/Specs/html-info/25306.htm.
13. *3GPP2 Specifications: cdma2000 High Rate Packet Data Air Interface Specification (TIA-856 Rev.A)*, 2005; http://www.3gpp2.org/Public_html/specs/tsgc.cfm.
14. *3GPP2 Specifications: cdma2000 High Rate Packet Data Air Interface Specification (TIA-856 Rev.B)*, 2009; http://www.3gpp2.org/Public_html/specs/tsgc.cfm.
15. "Packet Clearing House (PCH) - Internet Exchange Directory," 2010; https://prefix.pch.net/applications/ixpdir/.

16. "Verizon Global Network"; http://www.verizonbusiness.com/worldwide/about/network/maps/map.jpg.
17. "The Internet2 Network"; http://www.internet2.edu/network/.
18. Blue Coat Systems, "Blue Coat Publishes Annual Web Security Report"; http://www.bluecoat.com/news/pr/4372.
19. C. Shan, "Zeus Crimeware Toolkit | Blog Central," 2010; http://blogs.mcafee.com/mcafee-labs/zeus-crimeware-toolkit.
20. P. Coogan, "SpyEye Bot versus Zeus Bot | Symantec Connect"; http://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot.
21. The H Security, "Banking trojan ZeuS homes in on SMS-TAN process - The H Security: News and Features," 2010; http://www.h-online.com/security/news/item/Banking-trojan-ZeuS-homes-in-on-SMS-TAN-process-1097104.html.
22. R. Lemos, "Banking Trojans Adapting To Cheat Out-of-Band Security - Dark Reading Oct 18, 2011," 2011; http://www.darkreading.com/advanced-threats/167901091/security/client-security/231901086/banking-trojans-adapting-to-cheat-out-of-band-security.html.
23. K. Zetter, "Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target | Threat Level | Wired.com"; http://www.wired.com/threatlevel/2010/09/stuxnet/#ixzz10kcTAGUH.
24. Microsoft, "Microsoft Security Advisory (2718704) Unauthorized Digital Certificates Could Allow Spoofing," 2012; http://technet.microsoft.com/en-us/security/advisory/2718704.
25. NIST, *SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy*, 2009; http://csrc.nist.gov/publications/PubsSPs.html.
26. NIST, *SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, 2007; http://csrc.nist.gov/publications/PubsSPs.html.
27. A. Frier, P. Karlton, and P. Kocher, *The SSL 3.0 protocol*, 1996.
28. S. Kent and R. Atkinson, *RFC 2401: Security Architecture for the Internet Protocol*, 1998.
29. *IEEE Std. 802.1X-2004 IEEE Standard for Local and Metropolitan Area Networks— Port-Based Network Access Control*, 2004; http://standards.ieee.org/getieee802/portfolio.html.
30. "World Internet Usage Statistics News and World Population Stats"; http://www.internetworldstats.com/stats.htm.
31. techspot.com, "Internet to exceed 2 billion users this year - TechSpot News," 2010; http://www.techspot.com/news/40741-internet-to-exceed-2-billion-users-this-year.html.
32. "Network Centric Warfare: Background and Oversight Issues for Congress. CRS Report for Congress - Storming Media"; http://www.stormingmedia.us/50/5026/A502634.html.

PROBLEMS

I.1. If statistical multiplexing (SM) is used to provide Internet services, describe the ramifications of its use by an ISP when demand for bandwidth is high.

I.2. Explain the difference between transmission delay and propagation delay.

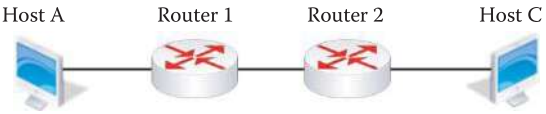
I.3. If a packet contains 100 bytes of headers (MAC, IP and TCP), 4 bytes of trailer for error detection, and 1000 bytes of payload, calculate the percent overhead (Indirect cost/Total cost) spent in delivering the 1000 byte payload.

I.4. If a packet contains 80 bytes of headers (MAC, IP and TCP), 4 bytes trailer for error detection, as well as 100 bytes of payload, calculate the overhead (%) involved in delivering the payload.

I.5. A packet contains 60 bytes of headers (MAC, IP and UDP header), a 4 byte trailer for error detection, and 100 bytes of payload. Determine the overhead (%) involved in delivering this information.

I.6. TCP's connection oriented approach requires a round trip for establishing a connection before delivering a file. If a file of 1000 bytes is sent over a link that has a 1.536 Mbps bandwidth and a 1 ms propagation delay, determine the overhead (%) involved in establishing a connection and sending the file from host A to host B. Neglect other delays.

I.7. Given the network shown in Figure PI.7 with destination host C connected to Router 2, determine the delay involved in sending a packet from host A to host C if the queuing delay is 0 and the remaining parameters are as follows:



PI.7

Packet length = 7 Kbits
Link rate R = 1 Mbps
Packet processing time = 0.001 s
Propagation speed s = 2×10^8 m/s
Distance between routers d = 2×10^5 m
Distance between router and host d = 0 m

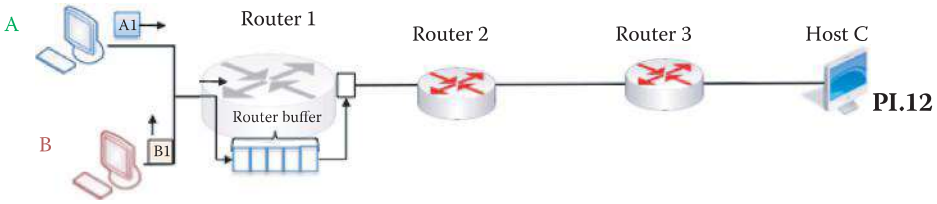
I.8. If a destination host C is connected to Router 2 as shown in the network in Figure PI.7, determine the delay involved in sending a packet from host A to host C given the following parameters and a router queuing delay of 5 ms:
Packet length = 7 Kbits
Link rate R = 1 Mbps
Packet processing time = 0.001 s
Propagation speed s = 2×10^8 m/s
Distance between routers d = 2×10^5 m
Distance between router and host d = 0 m

I.9. For the network shown in Figure PI.7, determine the delay involved in sending a packet from host A to host C given the following parameters:
Packet length = 10 Kbits
Link rate R = 1 Mbps
Packet processing time = 0.002 s
Propagation speed s = 2×10^8 m/s
Distance between routers d = 2×10^6 m
Distance between router and host d = 0 m
Queuing delay = 2 ms

I.10. If a destination host C is connected to Router 2 as shown in the network in Figure PI.7, determine the delay involved in sending a packet from host A to host C given the following parameters:
Packet length = 5 Kbits
Link rate R = 2 Mbps
Packet processing time = 100 μs
Propagation speed s = 2×10^8 m/s
Distance between routers d = 5×10^4 m
Queuing delay = 0.5 ms
Distance between router and host d = 0 m

I.11. Destination host C is connected to Router 2 in the network in Figure PI.7. Determine the delay involved in sending a packet from host A to host C given the following parameters:
Packet length = 3.1 Kbits
Link rate R = 155 Mbps
Packet processing time = 400 ns
Propagation speed s = 2×10^8 m/s
Distance between routers d = 5×10^3 m
Queuing delay = 800 ns
Distance between router and host d = 0 m

I.12. Given the network shown in Figure PI.12, in which destination host C is connected to Router 3, determine the delay involved in sending a packet from host A to host C if the queuing delay is 0 and the remaining parameters are as follows:



PI.12

Packet length = 7 Kbits
Link rate R = 1 Mbps
Packet processing time = 0.001 s
Propagation speed s = 2×10^8 m/s
Distance between routers d = 2×10^5 m
Distance between router and host d = 0 m

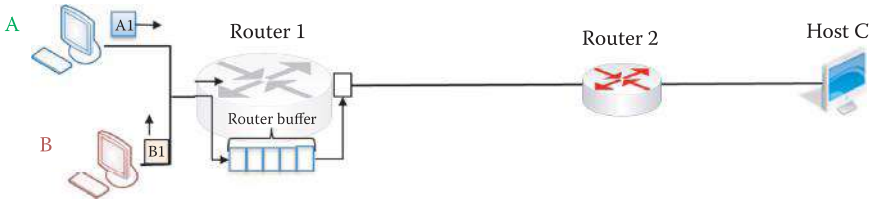
I.13. If a destination host C is connected to Router 3 as shown in the network in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters and a queuing delay of 5 ms:
Packet length = 7 Kbits
Link rate R = 1 Mbps
Packet processing time = 0.001 s
Propagation speed s = 2×10^8 m/s
Distance between routers d = 2×10^5 m
Distance between router and host d = 0 m

I.14. For the network shown in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters:
Packet length = 10 Kbits
Link rate R = 1 Mbps
Packet processing time = 0.002 s
Propagation speed s = 2×10^8 m/s
Distance between routers d = 2×10^6 m
Queuing delay = 2 ms
Distance between router and host d = 0 m

I.15. For the network shown in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters:
Packet length = 5 Kbits
Link rate R = 2 Mbps
Packet processing time = 100 us
Propagation speed s = 2×10^8 m/s
Distance between routers d = 5×10^4 m
Queuing delay = 0.5 ms
Distance between router and host d = 0 m

I.16. For the network shown in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters:
Packet length = 3.1 Kbits
Link rate R = 155 Mbps
Packet processing time = 400 ns
Propagation speed s = 2×10^8 m/s
Distance between routers d = 5×10^3 m
Queuing delay = 800 ns
Distance between router and host d = 0 m

I.17. Given the network in Figure PI.17 and the following assumptions and parameters, determine the time at which Host C receives the packet B1:



PI.17

Packet length L = 2 Kbits
Link rate R = 1 Mbps
Propagation speed s = 2×10^8 m/sec
Distance between routers d = 2×10^5 m
Propagation delay = d/s = $(2 \times 10^5$ m)/$(2 \times 10^8$ m/sec) = 0.001 s
Transmission delay = L/R = (2 Kbits)/(1 Mbps) = 0.002 s
Packet processing time = 0.001 s
Distance between router and host d = 0 m
A has 4 packets to send (A1, A2, A3, A4), B has 5 packets to send (B1, B2, B3, B4, B5) and the packets are sent in the sequence B1, A1, B2, A2,—etc.
Routers 1 and 2 have buffer space for 5 packets
A and B have infinite buffer space and their distances to the first router are assumed to be zero.
Assume UDP Transmission

I.18. Given the data in Problem I.17, calculate the time at which the packet A1 reaches Host C.

I.19. Given the network in Figure PI.17 and the following assumptions and parameters, determine the time at which Host C receives the packet B1:
Packet length L = 3 Kbits
Link rate R = 1 Mbps
Propagation speed s = 2×10^8 m/sec
Distance between routers d = 2×10^5 m
Propagation delay = d/s = $(2 \times 10^5$ m)/$(2 \times 10^8$ m/sec) = 0.001 s
Transmission delay = L/R = (2 Kbits)/(1 Mbps) = 0.003 s
Packet processing time = 0.001 s
Distance between router and host d = 0 m
A has 4 packets to send (A1, A2, A3, A4), B has 5 packets to send (B1, B2, B3, B4, B5) and the packets are sent in the sequence B1, A1, B2, A2,—etc.
Routers 1 and 2 have buffer space for 5 packets
A and B have infinite buffer space and their distances to the first router are assumed to be zero.
Assume UDP Transmission

I.20. Given the data in Problem I.19, determine the time at which packet A1 arrives at Host C.

I.21. Given the data in Problem I.19, determine the time at which packet B2 arrives at Host C.

I.22. Given the data in Problem I.19, determine the time at which packet A2 arrives at Host C.

I.23. Given the network in Figure PI.17 and the following assumptions and parameters, determine the time at which Host C receives the packet B1.
Packet length L = 3 Kbits
Link rate R = 1 Mbps
Propagation speed s = 2×10^8 m/sec
Distance between routers d = 2×10^5 m

Propagation delay = d/s = $(4 \times 10^5$ m)/$(2 \times 10^8$ m/sec) = 0.002 s
Transmission delay = L/R = (2 Kbits)/(1 Mbps) = 0.003 s
Packet processing time = 0.001 s
Distance between router and host d = 0 m
A has 4 packets to send (A1, A2, A3, A4), B has 5 packets to send (B1, B2, B3, B4, B5) and the packets are sent in the sequence B1, A1, B2, A2,—etc.
Routers 1 and 2 have buffer space for 5 packets
A and B have infinite buffer space and their distances to the first router are assumed to be zero.
Assume UDP Transmission

I.24. Given the data in Problem I.23, determine the time at which packet A1 arrives at Host C.

I.25. Given the data in Problem I.23, determine the time at which packet B2 arrives at Host C.

I.26. Given the data in Problem I.23, determine the time at which packet A2 arrives at Host C.

I.27. A house connected to the Internet uses a DSL modem with an average download rate 1.5 Mbps. If a 100 M-bit file is to be downloaded, what is the average time required?

I.28. A house is connected to the Internet through a cable modem with an average downstream data rate of 948 Mbps to the neighborhood with 500 users. If a 100 M-bit file is to be downloaded, what is the average time required?

I.29. A university is connected to the Internet via a 2.5 Gbps ATM circuit. The connection set-up time is 100ms. If a 100 M-bit file is to be downloaded, what is the shortest time required to download this file?

I.30. A university is connected to the Internet via a 2.5 Gbps ATM circuit. The time needed to set up a connection is 100 ms in order to download a 100 M-bit file. If the server is connected as shown in Figure PI.30, and the propagation speed in the ATM circuit is s = 2×10^8 m/sec, what is the shortest time required to download this file?

PI.30

I.31. A university is connected to the Internet using a 2.5 Gbps IP network. The router needs 1ms to route a packet, each packet is 10000 bytes long and a 100 M-bit file must be downloaded. Assuming there is no congestion in the network, the server is connected as shown in Figure PI.31 and the propagation speed in the network is s = 2×10^8 m/sec, what is the shortest amount of time needed to download this file?

PI.31

I.32. Solve Problem I.30 if the distance between the server and host is 2 km.

I.33. Solve Problem I.31 if the distance between the server and host is 2 km.

I.34. Solve Problem I.32 if the ATM data rate is changed to 1.5 Mbps.

I.35. Solve Problem I.33 if the link data rate is 1.5 Mbps.

I.36. Solve Problem I.30 if the ATM data rate is 1.5 Mbps.

I.37. Solve Problem I.31 if the link data rate is 1.5 Mbps.

I.38. Compare the results obtained from Problem I.30 with those of Problem I.37, and determine if there is a dominant factor in each problem, and if so what it is.

I.39. If statistical multiplexing (SM) is used to provide Internet services, describe the ramifications of its use by an ISP when demand for bandwidth is high.

I.40. Explain the difference between transmission delay and propagation delay.

I.41. If a packet contains 100 bytes of headers (MAC, IP and TCP), 4 bytes of trailer for error detection, and 1000 bytes of payload, calculate the percent overhead (Indirect cost/Total cost) spent in delivering the 1000 byte payload.

I.42. If a packet contains 80 bytes of headers (MAC, IP and TCP), 4 bytes trailer for error detection, as well as 100 bytes of payload, calculate the overhead (%) involved in delivering the payload.

I.43. A packet contains 60 bytes of headers (MAC, IP and UDP header), a 4 byte trailer for error detection, and 100 bytes of payload. Determine the overhead (%) involved in delivering this information.

I.44. TCP's connection oriented approach requires a round trip for establishing a connection before delivering a file. If a file of 1000 bytes is sent over a link that has a 1.536 Mbps bandwidth and a 1 ms propagation delay, determine the overhead (%) involved in establishing a connection and sending the file from host A to host B. Neglect other delays.

I.45. The Internet backbone consists of a group of regional ISPs.
(a) True
(b) False

I.46. Access networks are the links between ISPs.
(a) True
(b) False

I.47. The standards that control the use of the Internet are listed in what are called
(a) RFPs
(b) RFCs
(c) RFIs

I.48. Elements within the Internet core are typically interconnected with
(a) Wire
(b) Radio
(c) Fiber
(d) None of the above

I.49. The standards body for IETF is ICANN.
(a) True
(b) False

I.50. A LAN is connected to the hierarchical portion of the Internet via a
(a) Edge router
(b) Gateway
(c) All of the above
(d) None of the above

I.51. The connection between a residence and an ISP can be of the form
(a) Cable modem
(b) DSL
(c) FITL
(d) All of the above

I.52. The advantage of using a dialup connection to surf the Internet is that the phone can be used at the same time.
(a) True
(b) False

I.53. The advertised speed of the digital subscriber line is 56 Kbps.
(a) True
(b) False

I.54. The frequency range for an ordinary telephone is 0-4 KHz.
(a) True
(b) False

I.55. The technology that uses fiber into a neighborhood and then coax to individual homes is
(a) DSL
(b) DSLAM
(c) HFC
(d) None of the above

I.56. From the following, select the best technology for high speed communication:
(a) BPL
(b) FITL
(c) POTS

I.57. In an Ethernet LAN, hosts are connected to an Ethernet switch and operate at which of the following speeds?
(a) 10 Mbps
(b) 100 Mbps
(c) 1 Gbps
(d) 10 Gbps
(e) All of the above
(f) None of the above

I.58. Global ISPs are also known as Tier-1 ISPs.
(a) True
(b) False

I.59. Tier-1 ISPs are interconnected at IXPs.
(a) True
(b) False

I.60. Verizon and Level 3 Communications are examples of Tier-1 ISPs.
(a) True
(b) False

I.61. The number of layers in the U.S. DoD protocol stack is
(a) 2
(b) 3
(c) 4
(d) 5
(e) 6

I.62. The layer in the protocol stack that aggregates the media bits into, e.g., a frame is
(a) Physical layer
(b) Network layer
(c) Data link layer

I.63. The layer in the protocol stack that routes packets is the
(a) Data link layer
(b) Network layer
(c) Transport layer

I.64. TCP and UDP are handled by the following layer of the protocol stack
(a) Data link layer
(b) Network layer
(c) Transport layer

I.65. One or more protocols support each layer of the protocol stack.
(a) True
(b) False

I.66. Protocols are implemented only in software.
(a) True
(b) False

I.67. As a message at the host proceeds down the protocol stack, the destination IP address is added at the
(a) Transport layer
(b) Network layer
(c) Data link layer
(d) None of the above

I.68. The layer of the protocol stack at the source that is responsible for delivering packets to the transport layer at the destination is
(a) Transport layer
(b) Network layer
(c) Data link layer
(d) None of the above

I.69. The movement of bits in the physical transmission media is the responsibility of the
(a) Transport layer
(b) Network layer
(c) Data link layer
(d) None of the above

I.70. Routers operate at
(a) Layer 2
(b) Layer 3
(c) None of the above

I.71. In transmission from source to destination, the source has to know the IP address of the first gateway and uses which of the following to obtain the gateway's MAC address?
(a) ARP
(b) TCP
(c) SMTP
(d) None of the above

I.72. In contrast to a layer 2 switch, routers and layer 3 switches understand both MAC and IP addresses.
(a) True
(b) False

I.73. TCP is a best effort, unreliable data delivery service.
(a) True
(b) False

I.74. UDP is a good transport service for voice and video.
(a) True
(b) False

I.75. With circuit switching, packets may be lost, corrupted or delivered out of order.
(a) True
(b) False

I.76. When packet switching is used, the layer at the destination that is responsible for reassembling the packets in the correct order is the
(a) Data link
(b) Network
(c) Transport

I.77. In IP-based transmission, an IP unicast provides a mechanism for sending a single media stream to a group of recipients on the Internet.
(a) True
(b) False

I.78. Statistical multiplexing is an efficient method for packet switching.
(a) True
(b) False

I.79. Circuit switching is the best technique for bursty data while packet switching is best for voice and video.
(a) True
(b) False

I.80. Buffer overrun is a symptom of congestion that will trigger flow control.
(a) True
(b) False

I.81. When the speed of the incoming packets exceeds the link data rate which of the following may occur?
(a) Transmission delay
(b) Queuing delay
(c) Packet loss
(d) All of the above

I.82. One of the most devastating effects of malware is the fact that it can mutate.
(a) True
(b) False

I.83. Which of the following are categories of malware?
(a) Trojans
(b) Spyware
(c) Viruses
(d) Worms
(e) All of the above

I.84. Trojans that may contain other categories of malware can provide a backdoor for illegal access to a host.
(a) True
(b) False

I.85. Which of the following elements are placed at critical points within a system to protect vital assets?
(a) Firewall
(b) IDS
(c) IPS
(d) All of the above

I.86. Which of the following elements are used in a system to monitor traffic by inspecting the entire packet?
(a) Firewall
(b) IDS
(c) IPS
(d) All of the above

I.87. While a firewall will block traffic from the Internet to the internal network it does permit traffic originating in the DMZ to enter the internal network.
(a) True
(b) False

I.88. IDS/IPS is strategically located on the Internet side of the firewall in order to detect a wide range of attacks.
(a) True
(b) False

I.89. Encryption and authentication are protection mechanisms employed in the transmission media.
(a) True
(b) False

I.90. The approximate number of decades that the Internet has been in existence is
(a) 3
(b) 4
(c) 5
(d) 6