CHAPTER 1

Introduction to Networking

What, exactly, is the Internet? Basically it is a global network exchanging digitized data in such a way that any computer, anywhere, that is equipped with a node called a "modem" can make a noise like a duck choking on a kazoo.

— Dave Barry

Most of us would be lost without data networks.[1] Just a few short years ago, when computers were first starting to make their way into the business world, data sharing would normally have to be done by copying and then carrying the data from one PC to the next.[2] Today, the data is transferred from one user to the next in a fraction of a second. The growth that networking has undergone is remarkable. And it doesn't stop there. Every day there are new standards being proposed, new innovations being developed, and updates and changes to these being addressed.

Advances in technology are a fact of life. What needs to be considered is that any advance that requires the movement of data from one point to the next will need the services of a network to do so. This is why the world of networking has grown so much (and will continue to do so). With users transferring large amounts of data and the amount of that data growing at a exponential rate, there seems to be no end to the opportunities networks offer.

This chapter provides an introduction to networking. The intention is to provide you with a good foundation before we dive into the ''nitty-gritty'' of networking. In this chapter, we cover the history of networking, the TCP/IP and OSI reference models, standards organizations, as well as some discussions and definitions. The approach we took with the first chapter will hopefully be

[1] As a matter of fact, everyone would be affected in one way or another.

[2] A.k.a. sneakernet.

an enjoyable read, as well as set the tone for the rest of this book. We tried to make this an interesting base chapter, splitting up the boring parts as much as possible.

So, without further ado, welcome to our introduction to networking.

1.1 Networking: A Brief Introduction

```
Main Entry: net·work·ing[3]
Function: noun
1: the exchange of information or services among individuals, groups, or
institutions; specifically: the cultivation of productive relationships
for employment or business
2: the establishment or use of a computer network
```

A *data network* is a group of computers connected to one another by communication paths, as well as the standards that allow communication. A network can connect to other networks, allowing virtually worldwide communication between two endpoints. Many networks share information among one another, creating larger networks. Figure 1-1 is an example of a segment of a network.

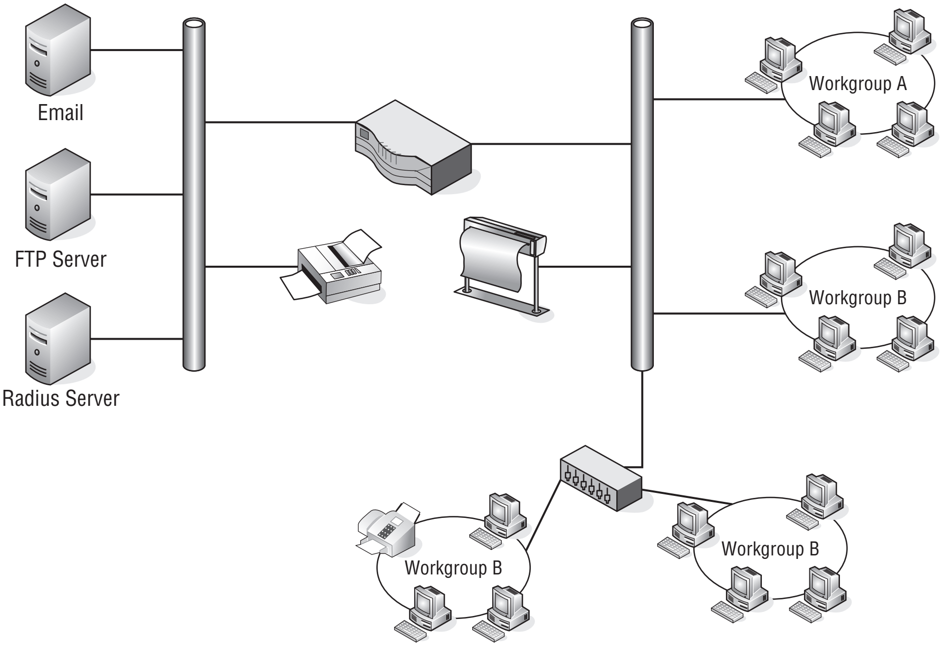


Figure 1-1 A computer network sharing applications as well as hardware

[3] *Dictionary.com Unabridged (v 1.1)*. Random House, Inc., accessed April 18, 2008.

Many things are shared on a network. Corporate business is conducted nearly exclusively on the network. Networks allow users to share applications that are stored on servers in the network (e-mail applications, word-processing applications, databases, and many others). They allow communication between end users. Data can be shared between companies or individuals for business or personal purposes. Many websites provide opportunities that would have not existed if networks had never been developed. Not to mention the entire file sharing that is enabled by a network. The possibilities are endless, and you can be sure that someone is working on a new, cutting-edge service even as you read this sentence.

Typically, networks are identified by their size. They range from small local area networks (LANs) to larger wide area networks (WANs).[4] Many networks remain isolated from others. They are there to perform tasks that fit the specific needs of the group or organization the network supports. These networks have in place networking standards that support the needs of their organization, without regard to anything outside of the network boundaries. This is due largely to the fact that upgrading (updating) the network can be a cost that the organization has not justified. If an organization does not need a high-speed LAN, why spend the money to upgrade to one?

ACRONYM ALERT

VPN — Virtual private networking

There are many other networks that have taken advantage of the tremendous technology breakthroughs in the past 25 years that enable these networks to share data securely. Vendors can connect to their clients' LAN to exchange business data in an instant. Internet service providers (ISPs) provide the gateway to the Internet for their customers to share information. We discuss many networking advancements throughout this book.

1.1.1 Internetworking

The ability to share information over dissimilar[5] networks is known as *internetworking*. By using a set of standards, nodes in two (or more) data networks can share information reliably between one another. In a bridged network,[6] the term does not really apply[7] as the data is not shared with multiple segments and no internetworking protocol is required to transfer the data.

Internetworking was designed for the specific purpose of providing an avenue for sharing data among different nodes on the network and among

[4] These are both discussed in depth in Chapter 2, ‘‘LANs, MANs, and WANs.’’

[5] By dissimilar, we mean networks that are running with different node types and/or standards.

[6] A collection of networks that are interconnected at the data link layer using network bridges.

[7] Although there are some people out there who insist the term does apply.

different system software and operating systems. Consider how data can be shared by the medical profession. Lab work can be returned more quickly, allowing for a more immediate diagnosis. Many hospitals are now allowing x-rays and other data to be viewed over a network. Remote offices are able to access this data in an instant, decreasing the time for a diagnosis to a level not even dreamed of 15 years ago. The possibilities are endless.[8]

Networking terminology can be a bit tricky, but it's really not as confusing as it may appear at first. Following are some of the more common terms[9] used to define networks of various purposes.

RANDOM BONUS DEFINITION

network application — A process or software program that runs on a node within a network.

1.1.1.1 [10] *An internet*

An internet (lowercase *i*) is a group of distinct networks connected to one another via a gateway.[11] ''An internet'' is often confused with ''the Internet'' (uppercase *I*), but an internet is not necessarily part of the Internet.

Basically, any network that conforms to the standards defined in the TCP/IP protocol suite (see Section 1.4) is an internet.

1.1.1.2 *The Internet*

> ***"A journey of a thousand sites begins with a single click."***
> **— Author unknown**

The Internet is what most people think of when they hear the term (upper- and lowercases aside). The Web, WWW, the Information Super Highway, and

[8] As a matter of fact, there is work ongoing that may allow a surgeon to log in from home and conduct an operation. Think how many lives can be saved because of this.

[9] As well as one that is outdated, but Jim just loves the word.

[10] Take a note of this number (not the section, the number). By the end of this book, you will know the significance of *all 1's*.

[11] As with many other networking terms, a gateway can mean many things. We are referring to a node capable of relaying user application information among networks employing different architectures and/or protocol suites.
Following are a few other definitions for the term *gateway* (for those of you who are interested):
(1) An internetworking node operating at the transport layer or above.
(2) An old term for an IP router.
(3) A marketing term for anything that connects anything to anything else.

many other terms define the network of networks. The Internet was developed mainly upon its predecessor, the Advanced Research Projects Agency Network (ARPANET). In addition to the Web, it encompasses a worldwide collection of networks, including academic institutions, government organizations, various public networks, as well as private networks (hopefully with the appropriate security measures in place).

SOMETHING YOU JUST HAVE TO KNOW

The Internet Protocol (IP) is the dominant standard used in networking to make sure that information is delivered from a source to a destination. We will talk about IP throughout this book, so it is not necessary to go into an in-depth definition at this point. You just have to understand that IP gets the data there.

1.1.1.3 Intranets (Give Me an "A", Remove My "E", Now Flip the "R" and the "A")

An *intranet* is an IP-based[12] network that is administered and controlled by a single entity. An intranet is a controlled network, with only users who have authorization to be on the network granted access to it (both remotely and physically onsite). A corporate LAN is an example of an intranet.

ACRONYM ALERT

LAN — Local area network

Although intranets are based on (and operate like) the Internet, they are not widely available to just anyone who needs to access them. Security is in place (firewalls, encryption and authentication measures, etc.) that will restrict access to only those who need the access. This allows remote users to access work applications over the Internet, while preventing unauthorized users from gaining access.

1.1.1.4 Extranets

An *extranet* is an intranet that is opened up to allow outside users (e.g., vendors, suppliers, employees, customers) access to the intranet (or any portion thereof). The access normally is provided by a server, which clients access over the Internet. An extranet operates securely to ensure that only authorized users are

[12] See! We told you that you would need to know what IP meant.

entitled access to the intranet. An extranet may comprise any of the following for security and privacy purposes[13]:

- **Firewall** — Network hardware and/or software that captures data passing through it and determines whether to pass or drop the data. Firewalls are configurable, and filters can be applied to provide the appropriate security for the LAN.
- **Public key certificate** — An electronic document that can verify and authorize an individual by public key cryptography. Public key cryptography uses two keys[14] (one public key and one private key) to encrypt and then decrypt data to ensure that a message can be transported securely.
- **Authentication encryption (AE)** — A system that is able to protect both the secrecy and the integrity of data communication.
- **Virtual private network (VPN)** — A network that is created when one network connects to another by a secure tunnel.

RANDOM BONUS DEFINITION

Tunneling is a method of securing access to an intranet. Another popular form is through a web server, where registered users can be authenticated after logging in through a web browser login page.

1.1.1.5 Virtual Private Networks

A virtual private network (VPN) is an extranet that securely connects separate networks to one another, as well as individuals to networks. VPNs updated[15] the use of dedicated lines that could only be used by one entity at a time. VPN technology is a much more proficient and cost-effective solution than the use of dedicated lines.

VPN technology uses a public network (normally the Internet) to connect users and networks to one another in what are known as *tunnels*. Data integrity is ensured by the use of security measures as well as tunneling protocols that set the rules for the tunnel.

VPN tunneling protocols include:

- Generic Routing Encapsulation (GRE)
- IP Security (IPSec)

[13] It's important to note that the technologies listed are not exclusive to extranets, but they are important technologies within extranets.

[14] A *key* is information used to determine an algorithm's output.

[15] Although many organizations now use VPNs (or some other extranet type) for remote access, some networks still utilize the dedicated lines (both owned and leased) when network access is required.

- Layer 2 Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)

Tunneling protocols ensure that the data is encrypted on the sending end of the tunnel and is decrypted appropriately at the receiving end of the tunnel. In addition to the data encryption, security is established to ensure that endpoint addresses are encrypted as well.

RANDOM BONUS DEFINITION

network node — Any device that participates in data communication within a network.

1.1.1.6 Catenet

The term *catenet* stands for ''catenated network.'' A catenet is simply a group of networks that are connected to one another via a gateway. It is an obsolete term that was replaced by some more up-to-date terms (i.e., internet) that we discuss in the pages that follow.

AND NOW, A MOMENT OF THOUGHT

Maybe someone will propose a standard to replace the word *internet* (lowercase *i*) with *catenet* and save us all that darn confusion. I mean, it really would make sense, right? However, should this ever happen, I would bet $20 that it wouldn't be long before "the Internet" became "the Catenet" and then we would be right back where we were before.

What it boils down to is that it would be nice to see the term *catenet* return. It's kind of catchy.

1.1.1.7 Area Networks

Chapter 2, ''LANs, MANs, and WANs,'' discusses area networks in depth. However, for those who may not have heard these terms, it is appropriate to have a brief introduction to area networks in this first chapter.

An *area network* is simply a network that spans a specific geographic area and serves a specific purpose. Any time you communicate over a network (wired or wireless), you are using an area network (or even various area networks and network types). In a nutshell, a LAN, a WAN, and a MAN are basically all the same. The differences are the geographical area that each covers, as well as some of the communication protocols that are in use.

POP QUIZ

What is a public key certificate?

The main three area networks you will probably hear about are the local area network, the metropolitan area network, and the wide area network. There are a few other area network terms in use at the time of this writing, but they are not referred to as often as the aforementioned. These less common area networks are the personal area network (PAN), the campus area network (CAN), and the global area network (GAN).[16]

1.1.1.7.1 Campus Area Networks

A network that spans a limited geographic area specific to academics is considered a campus area network (CAN). A CAN is nothing more than a MAN that connects university buildings and provides services for the staff of the university and its students.

Some CANs provide additional services such as classroom updates, labs, e-mail, and other necessary services for the students via iPod, cell phone, and other wireless technologies. You may or may not ever have to be involved in a CAN, but at least now you can share your CAN knowledge should the opportunity present itself.[17]

1.1.1.7.2 Global Area Networks

A global area network (GAN) is any network that connects two or more WANS and covers an unlimited geographical area. The entire network connected together would be considered a GAN. GANs are becoming increasingly popular as so many companies are opening offices and operating business on a global scale.

1.1.1.7.3 Local Area Network

A local area network (LAN) is a data network that covers a small geographical area, typically ranging from just a few PCs to an area about the size of an office building or a group of buildings. Unlike WANs, LANs don't require a leased line to operate. LANs also maintain higher data rates than do some of the larger area networks, due mainly to the smaller area of coverage.

Nodes that are members of a LAN communicate with other LAN nodes by sharing some form of channel (e.g., a wireless access point, twisted cable, fiber optic cable). PC users on a LAN often use a shared server to access and work with certain applications used by the organization.

[16] In the near future, you might see this one used a lot more. The use of the word *global* has increased over the past few years, so it stands to reason that a GAN is right around the corner.

[17] Or you can just sit on your CAN, er, knowledge and keep it to yourself.

The three major LAN technologies in use today are Token Ring (discussed in Chapter 7, ''Not to Be Forgotten''), Ethernet[18] (discussed in Chapter 6, ''Ethernet Concepts''), and Fiber Distributed Data Interface (FDDI), also discussed in Chapter 7.

1.1.1.7.4 Metropolitan Area Networks

A metropolitan area network (MAN) is a network that physically covers an area larger than a LAN and smaller than a WAN. The network is normally maintained by a single operating entity, such as government offices, healthcare systems, and any other type of large organization or corporation.

MANs allow communication over a large geographical area, utilizing protocols such as ATM, FDDI, Fast Ethernet, or Gigabit Ethernet.[19] This is a better solution than communication between LANs over a WAN, which relies on routing to decipher and allow communication of different protocol types between various area networks. Communication over a WAN is also slower and more expensive than what is offered by a MAN. MANs also provide control of the transmission of data from endpoint to endpoint, whereas the WAN solution requires that you rely on the service provider for a portion of the data flow control.

1.1.1.7.5 Personal Area Networks

A personal area network (PAN) is a network that is established for an individual user within a range of around 30 feet — for instance, a person has a PDA or cell phone and connects to a PC or other node for the purposes of exchanging data. This is done wirelessly, although wired PANs are feasible in this day and age. A pure wireless PAN is termed a WPAN, although most PANs would likely be made predominately of wireless devices. Although a PAN or WPAN might be considered a LAN or WLAN, the defined area outlined by the terms certainly does help in isolating network segments.

Some examples of devices that might make up part of a PAN include:

- iPhone
- Personal digital assistants (PDAs)
- Cellular phones

[18] Ethernet is by far the most popular and widely used LAN technology. As a matter of fact, many LANs are now migrating to Ethernet when they begin replacing legacy nodes in their LANs. Chapter 6, *Ethernet Concepts*, is dedicated to this technology.

[19] Although many MANs still utilize a lot of these various protocols (e.g., FDDI, ATM), Ethernet-based MANs are rapidly becoming the preferred standard. Most new MANs are Ethernet-based, and many MANs are migrating to the Ethernet-based solution as their MAN standard.

- Video gaming systems
- Pagers
- Personal computers or laptops
- Printers
- Most portable peripherals

1.1.1.7.6 Wide Area Networks

A wide area network (WAN) is a network that covers a large geographical area.[20] Most people think of a WAN as a public shared network, which is partly the case, but a lot of privately owned as well as leased WANs are currently in existence.[21] A WAN links other area networks to one another, providing a way to transmit data to and from users in other places. If you think about it, the WAN is the king of the area networks (although this might not hold true for much longer, as the GAN is quickly gaining speed to become the big daddy of them all).

WANs use networking protocols (e.g., TCP/IP) to deliver data from endpoint to endpoint. A WAN also ensures that addressing of endpoints is maintained so it knows where data needs to go to reach its intended destination. Some communication protocols that are used on WANs to handle the transmission of data include:

- Asynchronous Transfer Mode (ATM)
- Frame relay
- Packet over SONET (POS)[22]
- X.25[23]

1.1.1.7.7 Wireless Local Area Networks

A wireless local area network (WLAN) is an LAN without wires. WLANs use modulation technologies that are based on radio wave technology to allow communication with other wireless nodes within a limited geographical area.

Many businesses now offer WLANs for use by their customers (many at no charge). Additionally, many cities in the United States are implementing WLANS throughout their city to allow free access to users within the wireless area.

[20] You can consider a network a WAN if the network boundaries exceed the size of a large metropolitan area. But hey, one man's MAN is another man's WAN.

[21] These will not be going away. As a matter of fact, no one knows what the future holds. The possibilities seem endless.

[22] Here is another fun acronym to consider. Instead of Packet over SONET (POS), why not SONET under Packet (SUP)? Then when you greet your fellow networking professionals you could say, ''Hey! What's SUP?''

[23] X.25 is an oldie but goodie. It has long been replaced by other protocols. Still, it was one of the earliest WAN protocols and it deserved a mention.

1.1.2 Network Relationships and Topologies[24]

RANDOM BONUS DEFINITION

packet — The encapsulated data that is transmitted and received at the Network layer (see Section 1.4.2.5).

Network relationships refer to the communication that takes place between two nodes over a network. When a relationship is formed, the nodes are able to utilize resources between one another in order to share data. There are two network relationship types that define the foundation of any network. A *peer-to-peer* network relationship is where both nodes treat each others as equals, whereas a *client/server* network relationship is one in which one node (the server) handles storing and sharing information and the other node (the client) accesses the stored data.

The manner is which nodes in a network connect to a communication line in order to exchange data is an example of a *physical topology*. Another topology type would be a *logical topology*, which defines the way data is passed from endpoint to endpoint throughout the network. The logical topology does not give any regard to the way the nodes are physically laid out. Its concern is to get the data where it is supposed to go.

1.1.2.1 Network Relationship Types

ACRONYM ALERT

TCP — Transmission Control Protocol

The main difference between the two network relationship types are whether you want to have every user share resources with each other or have a central node that handles all the processing while serving the needs of the clients. This means that pretty much everything else is the same between the relationships. They both use the same protocols and physical connections to the network. Which one is appropriate for an organization depends on the needs, wants, and demands of the users of the network (cost factors, data speed concerns, etc.).

1.1.2.1.1 Client/Server Network Relationship

In a client/server[25] network relationship, one node acts as a server and the other nodes are clients that utilize the resources of the server to access an

[24] *Relationships and Topologies (RAT)*. Now, that acronym has a certain ring to it. Or maybe we should have written this heading to read *Network Relationships or Topologies (ROT)*. The former has a better ring, in our opinion, so *RAT* it is!

[25] A client/server network relationship is different from a client/server database system. In both cases, the server provides the data requested by a client, but in a database system, the client node has to use its own resources to format and view the data retrieved.

application or service. In a client/server network relationship, the server stores data (e.g., e-mail applications, encryption and authorization services, printers, VPN network access, and many more) that is used by the users of the organizational LAN. Most servers are Unix based, or a derivative of Unix, such as Linux or SunOS, all of which are discussed in depth in Chapter 4, ''Operating Systems and Networking Software.'' The users interface with the network through a PC or Mac (or whatever device is necessary at that time[26]). The PCs will have an application that contains the information necessary to connect to and share data with the server. Figure 1-2 shows an example of the client/server relationship.

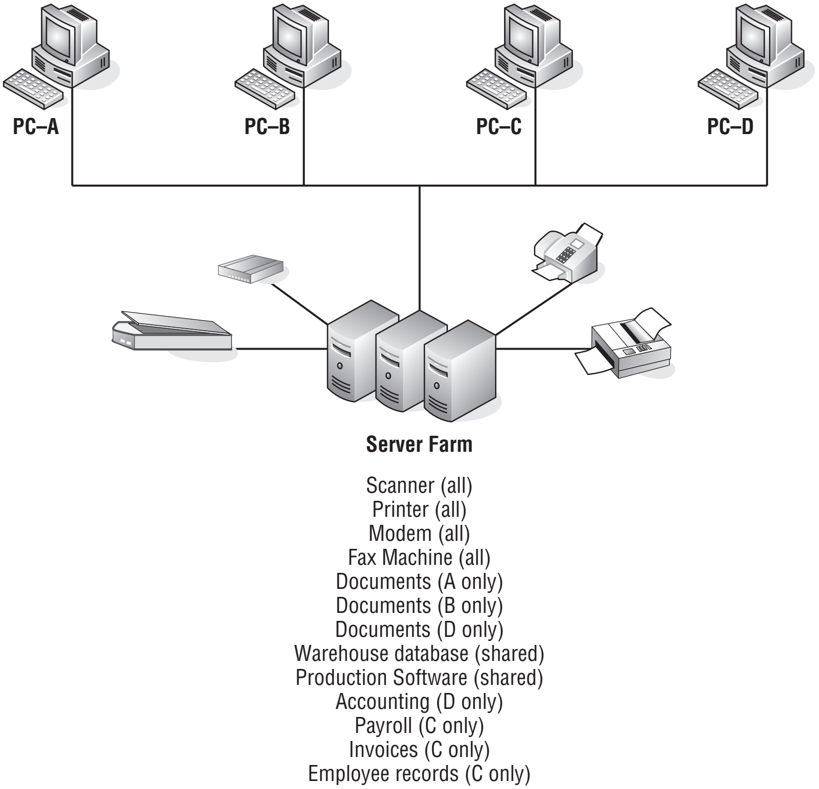


Figure 1-2 A client/server network relationship

No clients share resources with any other client in the client/server network relationship. They are simply users of the resources that are made available by

[26] For the remainder of the book, when a reference is made to a network user, it is assumed that the user is a PC end user. Otherwise, we will specify the type of user that is being referenced. Don't worry, Mac fans. Chapter 4, ''Operating Systems and Networking Software'' talks about the Mac OS.

the server. The servers maintain and provide shared resources to a specified number[27] of clients.

Advantages of a client/server network relationship include:

- It is a secure way to share data over a network. Because all the accessed resources are on the server, the server is able to control and maintain the security of sessions. Also, instead of multiple nodes in various locations, the server is a single entity and can be secured away from unauthorized visitors.
- Because most servers have more built-in redundancy than a single user's PC, the servers are very reliable in doing their job. Normally, there are backup drives (or other servers) that can be failed over[28] to if there is a problem with the primary drive or server.
- It is easier to back up data that is on the server than to do so with many nodes. Most organizations perform backups at night when the server is not as busy. Having only one node to back up makes it a very simple, time-saving process.
- Servers are fast because they have to serve multiple end users at the same time. The performance standards set for a server are far higher than the standards for a PC.

Of course, it's not all peaches and cream in client/server land. Disadvantages of a client/server network relationship include:

- Administrators of the server have to be trained and experienced. There is a lot to know, and the potential for failure is very high without a trained professional (therefore, be prepared to pay).

POP QUIZ

Encapsulated data that is transmitted and received at the Network layer is called a ______________.

- Servers require more physical resources in order to do the job. This makes the price to operate a bit higher than in a peer-to-peer environment.

1.1.2.1.2 Peer-to-Peer Network Relationship

A peer-to-peer network relationship is exactly that: all the users are peers (equals) and they share resources that are necessary to be shared. Each

[27] The total number would depend on the capabilities of both the server hardware and the software that it is running on the node.

[28] In a redundant configuration, a failover occurs when the primary has a failure and the backup has to take over as the primary. A failover is transparent to the end users.

computer is required to determine what is to be shared and then ensures that resources are made available to the nodes that need to access the resources. Figure 1-3 shows an example of how this works.

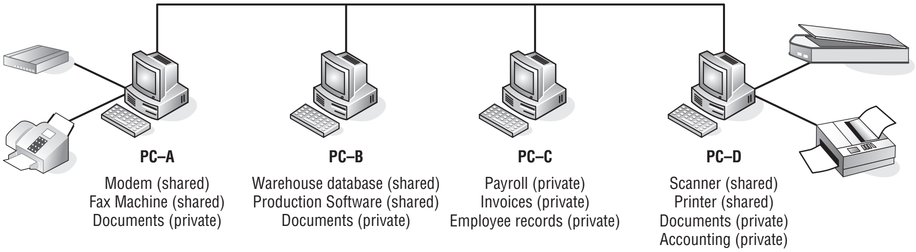


Figure 1-3 A peer-to-peer network relationship

Note that in the example, PC-C does not have any shared resources, but it may have a need to use some of the shared resources in the peer-to-peer network. Therefore, PC-C will be a part of the peer-to-peer topology as a user of the other resources made available by the other peers.

Some examples of shared resources include:

- Printers
- Modems
- Scanners
- Data files
- Applications
- Storage devices

A peer can share any of these in any combination that makes the best use of resources to meet the needs of the users in the network. One computer can provide access to the office printer and scanner, while another computer can have the modem connected to it. By sharing resources, you save the expense of having to have one of everything for every computer in the organization. Security for the shared resources is the responsibility of the peer that controls them. Each node will implement and maintain security policies for the resources and ultimately ensures that only those that have a need can use the resources. Each peer in a peer-to-peer network is responsible for knowing how to reach another peer, what resources are shared where, and what security policies are in place.

Advantages of a peer-to-peer network relationship include:

- It is cheaper to implement and maintain. You don't have to buy multiple peripherals for each computer. You also don't have the cost of purchasing and maintaining a server. Because each peer uses its own resources, there is no stress on only one node to do all the serving.

- A peer-to-peer network does not require a special operating system. A peer-to-peer network can be built on operating systems that are currently running on most PCs.
- There are more redundancy options available in a peer-to-peer network. Because multiple clients are sharing resources, it is a good idea to design a way to have a process failover to a backup peer should the master peer have a failure.
- A peer-to-peer network is easier to maintain than a client/server network, and the job of keeping up with the network can be assigned to multiple people.[29]

Disadvantages of a peer-to-peer network relationship include:

- If a lot of people are trying to use a shared resource, computer performance may be adversely affected.
- Because multiple peers are performing different tasks, it is harder to back up data in a peer-to-peer network.
- Security is not as good as in a client/server network. Because each peer is responsible for maintaining security for the resources it controls, the potential exists that an end user may accidentally or maliciously change the security parameters, causing a security lapse on that particular node. Also, each node is physically available to multiple people (possibly even people who work in the same building but whom you don't know). In a client/server environment, the administrator maintains security and the server is physically set apart from the clients.

1.1.2.2 Network Topology Types

A network *topology* is basically the way all the nodes in the network are connected. There are five primary topologies (bus, mesh, ring, star, and tree) that are installed in various networks. When designing a network, knowing which topology to use is determined by several factors:

- Is speed a concern?
- How reliable does the network need to be?
- How much money are you willing to spend to set it up?
- How much are you willing to spend to maintain the network?

[29] And where exactly does the buck stop?

Data is carried in the network by a detailed cabling scheme. How the network performs depends on whether the cabling is set up correctly.[30] Miss a port here or there and you can really cause a network some problems. If there is a cable that is longer than specifications, you are going to have other problems. Once you complete this section, you will come to realize that networking is more than just ''plugging it in.''

1.1.2.2.1 Bus Topology

The bus topology is probably the easiest one to understand and to implement. It is simply a topology in which all the nodes are connected to a single shared cable (called a *bus*). The cable is terminated at each end to prevent an open loop condition. Figure 1-4 shows an example of a bus topology.

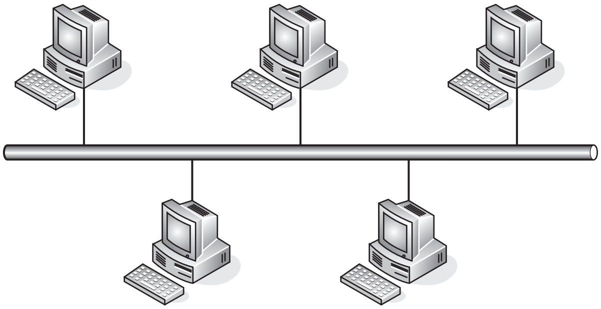


Figure 1-4 A bus topology

As with any of the topology types, the bus topology has benefits as well as drawbacks. The advantages of a bus topology include:

- It's easy to install and maintain.
- Adding new nodes is rather simple.
- Less cabling is required than with some of the other topology types.
- It's inexpensive to implement.

The disadvantages include:

- If the cable breaks at any point, network access is lost to all nodes on the segment.
- It can be expensive to maintain over a period of time.
- Data communication is slower than with some of the other topologies.

[30] When designing a network, the placement of the cabling is the first thing that you need to consider and then you expand from that. Of course, wireless networking is an option, but you still begin planning the wireless network by determining where the access points should be.

- The network segment traffic flow is affected each time a node is added.
- There is a limit to the number of nodes that can be added to the segment.

When a node that is connected to a shared bus needs to pass data on to the network, it has to have a mechanism for detecting whether other nodes are transmitting data at the same time. It must do this to prevent a collision on the bus (see Figure 1-5) or have a set of rules to follow when a collision occurs. In the example, you see that node C is trying to send data to node D. At the same time, node A is sending data to node E. Because there is no way to determine whether the other node was passing data, a collision occurs on the bus. This is not the worst part — because there was no mechanism within the bus topology to detect collisions, both of the sending nodes assume that the data reached the intended recipients and they relax, thinking they successfully sent the data.

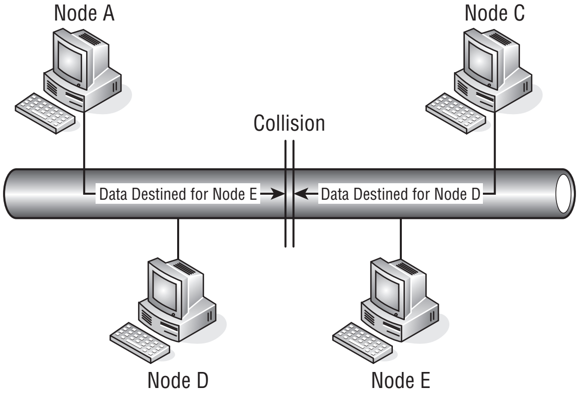


Figure 1-5 The dreaded collision

Collision avoidance can be handled in the following ways in a bus topology:

RANDOM BONUS DEFINITION

physical port — A physical interface that resides on a network node. Not to be confused with a TCP/UDP port.

- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol**[31] — This is a method of determining if another node is sending data by listening on the bus first. If it senses that the channel is being used by another node, the node will delay transmitting its data until the channel is available. CSMA is used to avoid collisions, while CD will detect

[31] Protocols are discussed in Section 1.1.3.

when a collision occurs and will stop transmitting data. Once a set period of time has lapsed, the sending node will send the data again. Take note that if CSMA is used without the CD, each sending node will send the entire *datagram*,[32] even when a collision occurs.

- **A bus master** — A bus master is an application running on one of the nodes within the segment or a separate node known as an *input/output (I/O) controller*. The bus master is the master node and all other nodes are referred to as slave nodes. The master controls the transmission of data to and from all nodes within the bus topology.

RANDOM BONUS DEFINITION

TCP/IP port — A number in the data packet header that maps to a process running on a node. Not to be confused with a physical port.

1.1.2.2.2 Mesh Topology

There are two types of mesh topologies that can be used. A full mesh topology (Figure 1-6) is a configuration where all the nodes within the network segment are connected to one another. A partial mesh topology (Figure 1-7) is where some nodes are connected to all the others, and some only connect to the ones they need to communicate with.

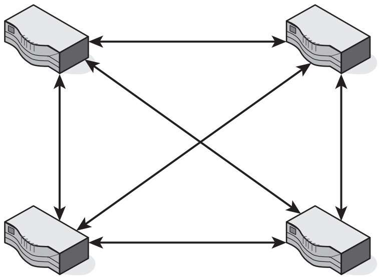


Figure 1-6 A full mesh topology

As with almost any topology, there are some advantages and some disadvantages to the mesh topology. One advantage of the mesh topology is that you have a lot of redundancy. If one node is down, the others are virtually unaffected. There is always a route around broken or blocked paths.

[32] A *datagram* is a self-contained entity of data that is transmitted from one endpoint to another within a network. Layer 3 packets and Layer 2 frames are two examples of datagrams. As a matter of fact, many network professionals use the three terms interchangeably.

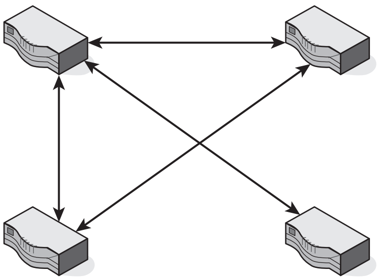


Figure 1-7 A partial mesh topology

One major disadvantage of the mesh topology is that it is expensive to implement. Also, as the network grows, so does the complexity of the mesh topology. In Figure 1-6, there are four nodes within the mesh topology. Imagine what a nightmare it would be to maintain a mesh that included 100 nodes.

ACRONYM ALERT

FTP — File Transfer Protocol

1.1.2.2.3 Star Topology

The star network is one of the more popular network types used by organizational LANs. In the star topology, all nodes in the network connect to a central node that handles the passing of datagrams between the nodes. Figure 1-8 shows an example of the star topology.

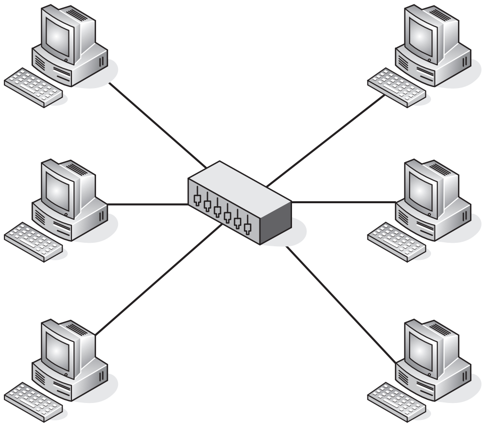


Figure 1-8 A star topology

The central node receives a datagram and then broadcasts the data to all the nodes it connects to. The connecting nodes can communicate with each other by sending data to and receiving data from the central node. Should one of the connecting nodes go offline, the central hub will discontinue communication to the one node only and the other connecting nodes will continue to operate.

The advantages of a star topology include:

- It allows for direct communication between two nodes.
- It's simple to implement and maintain
- It helps to narrow down problematic network segments.
- It's easy to troubleshoot and allows for quick recovery.[33]

The disadvantages include:

- If the central node fails, all the other nodes are affected.
- If there is an increase in network traffic, the central node may become ''sluggish,'' affecting the performance of some, if not all, of the connecting nodes.
- Scalability within the network is limited to the capabilities of the central node.

1.1.2.2.4 Ring Topology

The ring topology can be a bit confusing, as the term *ring* defines the logical topology rather than the physical topology. As shown in Figure 1-9, the ring passes data logically from station to station until the data reaches its destination.

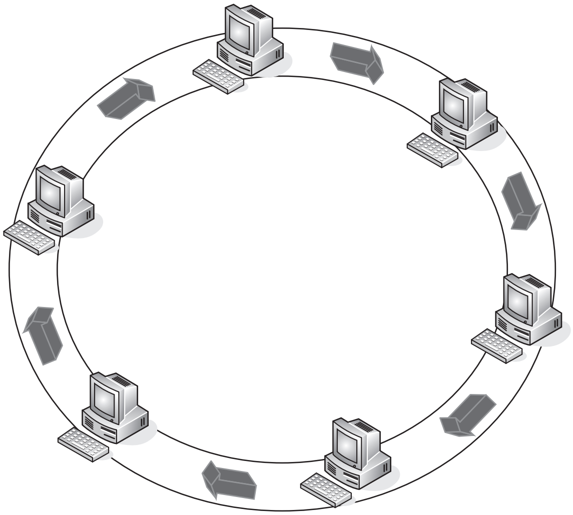


Figure 1-9 A ring (logical) topology

[33] When the problematic link is discovered, all you have to do is pull out the cable to prevent the issue from propagating to the rest of the nodes within the star.

Each node handles each datagram that is passed, verifying whether the datagram is destined for it and, if not, passing it along to the next node. In the ring topology, there is a single path from one node to the next. Should there be a break along the way, all nodes on the ring will no longer be able to communicate on the network. To overcome this, many ring topology networks employ a dual ring, with data passing in the opposite direction on a redundant ring (see Figure 1-10).

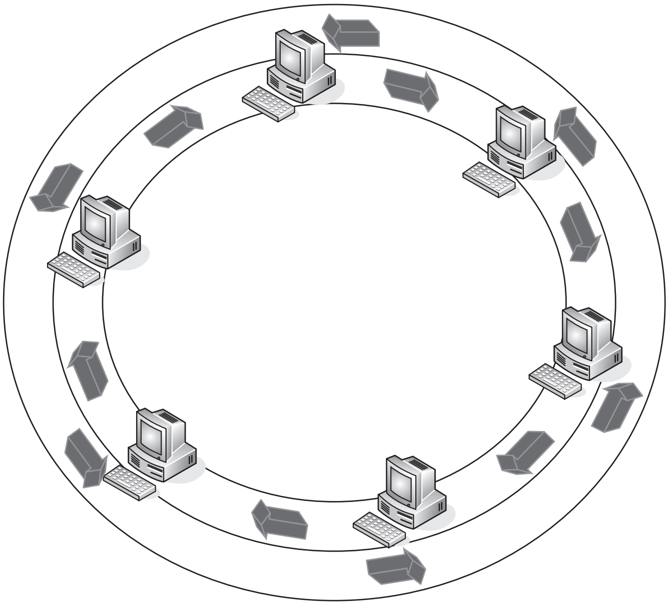


Figure 1-10 A dual-ring topology

Advantages of a ring topology include:

- There's no need to have a mechanism to ensure collision-free datagram passing.
- It can expand to cover a greater number of nodes than some of the other topology types.
- It's fairly simple to maintain.

Disadvantages of a ring topology include:

- A failure with one node on the ring may cause an outage to all connected nodes.
- Any maintenance (e.g., adding a node, making a change to a node, removing a node) would affect all the nodes that connect to the ring.
- Some of the hardware required to implement a ring is more expensive than Ethernet network cards and nodes.

- Under normal traffic load, a ring is much slower than other topologies.
- There are not many of this type of network, as most networks are migrating to Ethernet.

1.1.2.2.5 Hierarchical Topology (a.k.a. Tree Topology)

A hierarchical[34] topology is very similar to a star topology. Like the star topology, the hierarchical topology has a central node that connects multiple nodes to one another. However, in the hierarchical topology, each node could potentially act as a central node to a group of other nodes. Figure 1-11 shows the physical layout of a hierarchical topology.

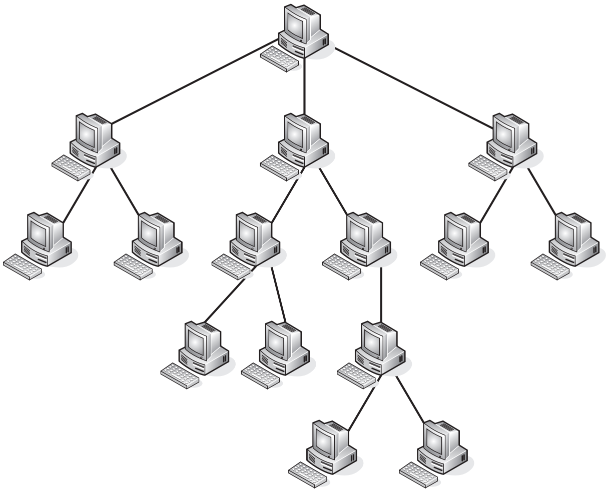


Figure 1-11 A hierarchical topology

Notice how a hierarchical topology is similar to an organizational structure. The mainframe computer would be the single node at the top of the chart, and then the lower levels would be other minicomputers and PCs. The hierarchical topology is quite effective in smaller areas, where a central mainframe can connect to different minicomputers, and the minicomputers can provide a central connection for the PCs in the departments they serve.

1.1.3 Protocols

Simply put, a *protocol* is a standard (or set of standards) that governs the rules for setting up a data connection, communicating between endpoints once the connection is set, and transferring data between those endpoints. There are

[34] Jim used to have a colleague who could never get the pronunciation right for the word ''hierarchical.'' He would pronounce the word ''harr-arrr-cul-cul.'' No matter how hard he tried, he never could get the word down. It was pretty funny.

protocols set for both hardware and software, and sometimes for the combination of the two.

POP QUIZ

What is the difference between a physical port and a TCP port?

Network protocols vary in purpose and complexity. They are usually used to detect the physical properties of both the sending and the target nodes, as well as whether the target node is available. Once the connection endpoints are determined, a protocol will handle the initial communication[35] between the endpoints as well as the rules for the connection. The protocol will identify how each end will know where a data stream starts and stops, what format it will be sent and received in, and what to do with the data if there are any problems with the transfer.

The Internet would not be what it is if it were not for the protocols, especially the Internet Protocol (IP) and the Transmission Control Protocol (TCP), used in combination with each other and referred to as TCP/IP or the TCP/IP protocol suite.

TCP/IP and many other protocols are discussed throughout this book, but here is a short list of a few of the more common protocols:

- **File Transfer Protocol (FTP) —** FTP is used to transfer large amounts of data from one node to another. The FTP protocol uses an FTP server to serve files to an FTP client.
- **Hypertext Transfer Protocol (HTTP) —** HTTP is a communications protocol that allows for data transmissions within data networks as well as the World Wide Web (WWW). HTTP uses a server (e.g., a website) to serve the clients (end users) data the clients have requested via a web browser.
- **Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) —** HTTPS is an enhancement to HTTP that allows secure sessions over SSL. These sessions provide adequate security for private transactions on the WWW.
- **Internet Message Access Protocol version 4 (IMAP4) —** IMAP4 is a protocol that allows a client to connect to and retrieve e-mail from an e-mail server.
- **Internet Protocol (IP) —** IP is a standard that allows for the transfer of data between nodes that are connected on a network. Each node within an IP network has a unique address that identifies it for the purpose of locating and sharing data between nodes. The latest version of IP that has been released is IPv6.

[35] The initial conversation between the two endpoints is commonly referred to as a *handshake*.

- **Post Office Protocol version 3 (POP3)** — POP3 is a protocol that allows an e-mail client to connect to an e-mail server and retrieve mail that is destined for that client.
- **Simple Mail Transfer Protocol (SMTP)** — SMTP is a protocol that allows a network user to send and receive e-mail.
- **Simple Network Management Protocol (SNMP)** — SNMP is a protocol that allows for the sharing of management data on a network. SNMP allows network administrators the ability to quickly access network nodes to monitor performance, troubleshoot, baseline, and ensure that the network is capable of addressing the needs of the organization.
- **Transmission Control Protocol (TCP)** — TCP is a protocol that connects end users with one another and ensures the integrity of the exchanged data.
- **Trivial File Transfer Protocol (TFTP)** — TFTP is a protocol that is a simpler form of FTP.
- **User Datagram Protocol (UDP)** — UDP is a protocol that connects end users to one another and transfers datagrams, but does not ensure the integrity of the datagrams.

1.1.3.1 Transmission Control Protocol

The Transmission Control Protocol (TCP) ensures that data is transmitted from endpoint to endpoint in a reliable manner. TCP operates at the Transport layer of the OSI reference model (more on this in Section 1.4). TCP is normally associated with the TCP/IP protocol suite; however, it is its own entity. It is a protocol that can adapt to a variety of data delivery standards, providing reliable data delivery.

TCP is the reliable[36] transport protocol that controls the flow of data between hosts. TCP divides messages into smaller segments and ensures the data arrives error-free and is presented by the target node in the correct order. TCP manages the flow of data and makes adjustments to the size and the speed in which the data is transported. TCP is used by most of today's more popular networking services and applications, including the World Wide Web (WWW), e-mail, and Secure Shell (SSH).

[36] The key word here is ''reliable.'' This does not imply that TCP can provide the quickest delivery available. TCP is designed to offer reliable and accurate delivery, but it does not guarantee timely delivery and is not used when speed is needed to transmit data. The Real-time Transport Protocol (RTP) is normally used in these instances.

TCP is a connection-oriented protocol. This means that there is a connection between two endpoints before any data is sent. A connection-oriented protocol also ensures that once the data arrives at a destination, it is put back together in the proper order. A connection-oriented protocol cannot promise that data won't get dropped, but if it is received, it will be sequenced appropriately.

1.1.3.2 User Datagram Protocol

The User Datagram Protocol (UDP) provides a method for transmitting datagrams between endpoints, but no guarantee of the delivery is made. This means that a datagram may be duplicated, can go missing, and may not arrive in the order in which it was sent. This also means that UDP is a faster transmission standard than TCP.

UDP is preferred in situations where you need data to be transmitted quickly. There is simply more processing power to get the data to the destination because there is no error checking. UDP supports broadcasting[37] and multicasting,[38] so messages can get to destinations within a network segment as well as to everyone within the network.

UDP is a connectionless protocol, which means there is no guarantee that the intended destination is available. There is no checking the communication line prior to transmitting data, it is just transmitted.

1.1.3.3 Internet Protocol

The Internet Protocol (IP) is the protocol that defines how data is transmitted between two nodes. Datagrams are forwarded to a destination endpoint based on the IP address that is assigned to the endpoint. When data is transmitted, the data is encapsulated into datagrams and multiple datagrams may be required to transmit a single message. Each datagram is treated as its own entity without regard to any of the other datagrams that make up the message. Each datagram can choose whatever path it wishes to take to reach a destination. That is IP's job: to get the datagram to the destination by the quickest route possible.[39]

POP QUIZ

Because IP does not establish a connection before sending data to an endpoint, it would be considered a ______________ protocol.

[37] Sending data to everyone connected to the network segment.

[38] Sending data to a select group of nodes.

[39] It is TCP's job to put them back together again.

1.2 History of Networking

On April 3, 1860, the Pony Express officially opened for business. Covering 250 miles in each 24-hour period, the riders would travel at full gallop from one Pony Express station to the next. At each stop, they would change horses, exchange mail, and head on to the next stop. After 100 miles or so, the rider would be relieved by a fresh rider to continue the journey. What an accomplishment this was. Only 15 years prior to that, it would take six months to get a message from the east coast to the west coast. The Pony Express could do it in about 11 days. The Pony Express dissolved in October 1861, when the first transcontinental telegraph was transmitted.

Now look where we are today. In milliseconds, we can send a letter from Hong Kong to New York, or talk over the Internet with a loved one on the other side of the planet. We can get trip directions, listen to a radio station anywhere in the world, work, and play games — all at the same time. It is amazing how far communication has come.

It might surprise you to know that the concept of connecting nodes to one another was developed as a way for research organizations and educational institutions to share resources. There was one significant event that occurred that opened the doors for a lot of various research, some of which eventually introduced the network concept. What exactly was this event? It was the race to space.

The Soviet Union launched the Sputnik satellite on October 4, 1957. This alarmed many American citizens and was an embarrassment to many people in the United States because of a few failed attempts prior to that date. The launch of the Sputnik satellite is said to have ushered in the Space Age, but that is not all it changed. It changed the attitude of those who were involved in the United States space program, as well as the attitude of U.S. citizens. After Sputnik launched, funds began flooding to research agencies and institutions. The National Defense Education Act was signed to promote studies in math, science, and foreign languages. One of the agencies formed was the Advanced Research Projects Agency (ARPA) in 1958.

ARPA was formed as an agency that would be tasked by the United States Department of Defense (DoD) to research and develop projects. ARPA was not required to focus on only projects of military concern, and it was quickly determined that a focus on computers would be a worthwhile investment. In 1962, ARPA chose Dr. J.C.R. Licklider to lead the computer research effort.

WHAT'S IN A WORD?

If you think that the whole catenet/internet/Internet terming conventions seem a little confusing, you haven't seen anything yet. Check this out:

(continued)

WHAT'S IN A WORD? *(continued)*

The Advanced Research Projects Agency (ARPA) was formed in 1958. In 1972, ARPA was replaced by the Defense Advanced Research Projects Agency (DARPA). DARPA did the same job that ARPA did, but DARPA was established as a separate defense agency (still under the Secretary of Defense).

In 1993, DARPA became ARPA and was put back as it was when it was first formed. In 1996, the name was officially changed to DARPA again.

Licklider realized even before his appointment the potential of connecting nodes to one another to share resources. He had developed what he called a *galactic network* concept, and he was able to convince other researchers (including those who took over when he left) how important his concept was. He outlined his plan to accomplish this concept and the very first large network research team was formed. This team, known as the *ARPA community*, was a group of universities across the United States. It is important to note that Licklider left his position before his concepts became a reality, but his successors moved ahead in their development.

ARPA formed a subgroup called the Information Processing Techniques Office (IPTO) to focus on research pertaining to anything related to computing. It was funding from ARPA/IPTO that assisted in the ARPA community of educational and scientific institutions to investigate time and resource sharing possibilities.

POP QUIZ

What is the difference between a WAN and a LAN?

Many people today still feel that the Internet was developed to provide a fallback mechanism in the event of a nuclear attack. This is probably due to the fact that there was so much funding poured into development after the launch of the Sputnik satellite. The official reason that was given for the concept of networking nodes together was simply to share files and resources among investigative agencies and groups.

In 1968, ARPA allowed contractors to bid on the plan they had been working on, and BBN Technologies was brought in. In 1969, ARPANET was born. The original ARPANET was a network with several small computers referred to as *interface message processors* (IMPs), which were nodes that performed packet-switching and were used to connect to each other by modems and to users on host computers.[40] The IMPs were configured with 24 Kb[41] of memory,

[40] Don't think of these hosts as PCs. These hosts were huge computers, sometimes occupying a whole floor of a building.

[41] Kb = kilobits

supported up to four host computers, and were able to connect to a maximum of six other IMPs. The IMPs communicated with one another over leased communication lines. The original ARPANET was made up of four IMPs that were established at the following locations:

- Stanford Research Institute
- University of California, Los Angeles
- University of California, Santa Barbara
- University of Utah

BBN Technologies developed the first communications protocol, known as the *BBN Report 1822*, which later became known as the *1822 protocol*. The 1822 protocol simply specified the manner in which a host communicated with the IMP. The 1822 protocol predated the OSI reference model (see Section 1.4) and did not really follow the layering process we use today.[42] The 1822 protocol was eventually replaced by the Network Control Protocol (NCP), which incorporated a transport function. The NCP remained the main communication protocol until 1983, when it was replaced by the TCP/IP protocol suite. The TCP/IP protocol suite was more resilient than the NCP, and its introduction was the birth of communication networks as we have known them to date.

ACRONYM ALERT

DoS — Denial of service

Eventually, ARPA got out of the networking business to focus on research in other areas. The Defense Department retained the military portion of the ARPANET and named it the MILNET. The remainder of ARPANET remained with research and educational organizations, and BBN Technologies continued to maintain these networks. Because of the split of ARPANET, many of the resources available to the institutions and organizations were severed in the interest of security required by the MILNET. In response to this, the National Science Foundation funded the development of the Computer Science Network (CSNET), which provided access to shared resources for these groups. Eventually, the network grew and was transformed into the National Science Foundation Network (NSFNET), which was developed originally to allow researchers access to five supercomputers at the following locations:

- Cornell University
- Pittsburgh Supercomputing Center

[42] It can be said that the 1822 protocol used the physical, data link, and network layers as the host system packaged data and sent it to the address of the IMP (directly connected). The IMP, in turn, routed the data to the destination IMP, which sent it to the destination host.

- Princeton University
- University of Illinois
- University of California, San Diego

The NSFNET used the TCP/IP protocol suite as a communications protocol and was completely compatible with the ARPANET. In the early 1990s, more and more organizations started accessing what was now called the Internet, but permissions had to be obtained from the NSFNET to use many of the services that were offered. The main supercomputer centers maintained and monitored the Internet's growth.

Today networks are defined by the way they get information from point to point. The nodes used and the standards deployed are integral parts of any network, defining the very basis for that network's existence. Networks are commonplace and growing on a global level. Only the future can tell what new advances will be made for this global communication vehicle.

INTERNET TIMELINE TRIVIA

1957: The Advanced Research Projects Agency (AARPA) is formed.

1961: The Massachusetts Institute of Technology (MIT) began researching data-sharing potential. There are fewer than 9,500 computers in the world.

1966: ARPANET is under development, packet-switching technology is launched.

1969: ARPANET is launched.

1971: The number of nodes on the ARPANET is 15.

1973: London and Norway join ARPANET. Global communications are launched.

1974: TCP is launched. Data communication speeds increase and the reliability of data transmission improves.

1975: The first ARPANET mailing list is launched. TCP tests are run successfully from the U.S. mainland to Hawaii as well as to the U.K., via satellite links.

1976: Unix is developed.

1978: TCP and IP split into two separate protocols.

1982: TCP/IP becomes the standard used by the Department of Defense for data communication within the U.S. military's network.

1984: The number of nodes on the Internet is over 1,000. Domain Name Service is launched.

(continued)

INTERNET TIMELINE TRIVIA *(continued)*

1987: The number of nodes on the Internet is over 10,000.

1988: The Internet experiences its first Internet worm.

1989: The number of nodes on the Internet is over 100,000.

1990: ARPANET is disbanded. The first commercial Internet service provider (ISP) is launched.

1991: The first Internet connection is made (at 9600 baud). The World Wide Web is launched.

1992: The number of nodes on the Internet is over 1,000,000.

1994: The WWW becomes the most popular service on the Internet. Some radio stations start broadcasting over the Internet.

1995: Internet streaming technology is introduced.

1996: Web browser software vendors begin a "browser war."

1997: Over 70,000 mailing lists are now registered.

1998: The 2,000,000th domain name is registered.

2000: The first major denial-of-service (DoS) attack is launched. Most major websites are affected.

2002: Blogs become cool.

2003: Flash mobs are born. Flash mobs are groups of people who gather online and plan a meeting in a public place. Once they assemble, they perform a predetermined action, ranging from pillow fights to zombie walks. The participants leave as soon as the meeting is over. (Wikipedia has a good article about flash mobs: `www.wikipedia.org/wiki/Flash_mob`.)

2005: The Microsoft Network (MSN) reports that there are over 200 million active Hotmail accounts.

2006: Joost is launched, allowing for the sharing of TV shows and video using peer-to-peer technology.

2008: Online search engine Technorati reported that they are now tracking and indexing over 112 million online blogs.

1.3 Standards and Standards Organizations

As we have discussed already, the standards that are put in place to ensure that data communication can be shared between nodes on a network are an essential part of the network. Without a standard way of doing things, networks would not be able to operate nearly as efficient as they do today.[43] So it is fair to say that based on what we have discussed so far, we can all be in agreement that standards are required in order for data communication to be shared on a network. Standards serve the following purposes:

- Set up and maintain rules to be followed in the network
- Define how network hardware interfaces operate
- Maintain all communication protocols that are in use in a network
- Offer the ability of utilizing the hardware and software available from multiple vendors and ensure that these are interoperable with like resources from other vendors

Standards begin when an individual or organization has an idea. A proposal is put forth and a committee reviews it to determine if the proposal has any merit. If the proposal is accepted, the idea will be transferred to a development committee, which will outline the scope of the proposed standard and submit a draft to a committee that will vote on whether the standard is to be approved. If the standard is passed for approval, the final draft is written and then published as a new standard.

There are three main types of networking-related standards. It important that you understand the differences, as it is virtually a guarantee that you will need to know this at some point.

- **De facto standards** — A de facto standard is a standard that began as a proprietary standard and then grew to a standard that is used by pretty much everyone. As a matter of fact, it is widely assumed that many proprietary standards are developed with the hopes that they will become de facto standards.[44] A de facto standard is similar to an open standard in that it is universally used by multiple vendors, but it is never approved as a formal open standard.
- **Proprietary standards** — A proprietary standard is a standard that is developed and owned by a specific vendor. When PCs first started coming out, most vendors tried to avoid admitting the importance of a cooperative standard that could be used between different vendors. The technology was starting to boom, and corporate confidentiality was a huge concern, so it was important to keep their standards to themselves. As a matter of fact, it really made sense that having control of a standard

[43] That is assuming that they would work at all without standards.

[44] Why would they do this? To become the industry leader for whatever the standard covers. Think about it this way. If you want to purchase a computer that supports the widget standard, you might have more faith in the company that introduced and has supported the standard for years, as opposed to purchasing a PC from ''Mom and Pop's PC shop,'' which only recently started supporting the widget standard.

as it would be beneficial to the future of the company. To take this even further, companies saw no real value in supporting the proprietary standard of the competition (why have to pay them for the rights to use the standard?), so instead they developed something close to what the competition had, and then encouraged the consumer to move to what they had to offer, as they did ''xyz''[45] more than the competitor. Proprietary standards still exist, but they are not as common as they once were.

- **Open standards** — An open standard is a standard that is used by almost everyone. Most vendors involved in networking resources now realize that they can be just as competitive while developing cooperative standards that are agreed upon by other vendors. This quickly became evident as consumer demand grew. Consumers wanted to be able to choose from multiple vendors, and expected the nodes to communicate well with one another. There are some companies that still prefer to work with mostly proprietary standards, but there is a larger customer base for devices that use open standards.

ACRONYM ALERT

IEEE — Institute of Electrical and Electronics Engineers

This section discusses some of the standards organizations and what purpose each one serves. These organizations develop formal standards for the area of networking they are applicable to. Most standards committees operate as nonprofit organizations and are made up of researchers, educators, specific vendors, and industry professionals. In turn, vendors model the development of their products based on the agreed standard.

1.3.1 American National Standards Institute

The American National Standards Institute (ANSI) is the organization responsible for ensuring that guidelines are established for every type of business you can imagine. From construction standards to agricultural standards, ANSI is responsible for outlining and accrediting these standards. The mission of ANSI is to ensure that standards are defined and followed in order to protect and ensure global competitiveness

POP QUIZ

The three types of standards are ______________________________,
______________, and ______________.

[45] This could be anything from a true advance over the competitor to a ''prettier'' package.

for American business and ultimately improve life standards for the American consumer.

ANSI is the organization that represents the United States in working with the global community on issues relating to two important global standards organizations. These are:

- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)

It is important to note that ANSI is not the developer of standards; rather, it oversees the development of standards by accrediting the standards once they have been set up and proposed by what are known as Standards Development Organizations (SDOs). It is the responsibility of the SDOs to develop and maintain standards that represent the users for their group.[46]

Examples of some of the SDOs that have had standards accredited by ANSI[47]:

- American Dental Association (ADA)
- North American Die Casting Association (NADCA)
- Standards Australia (SAI)
- Institute of Electrical and Electronics Engineers (IEEE)
- Chinese Standards (SPC)

RANDOM BONUS DEFINITION

working group — A group formed by interested members of an organization. The working group can have open meetings, as well as communication through Internet forums and mailing lists. The working group works on issues relating to standards and standards development.

1.3.2 International Organization for Standardization

Founded in 1947, the International Organization for Standardization (ISO)[48] is an organization that is tasked with standardizing international standards for various interests. Based in Switzerland, the ISO is made up of members

[46] By ''group,'' we mean the individuals outside of the SDO for whom the developing standards will apply.

[47] This list is provided as an example of the broad range of communities that are ANSI accredited. That being said, some of these have nothing to do with networking. If you are interested in further reading, you can go to the ANSI website (`www.ansi.org`), or there is a search engine you can use to locate standards and SDOs (`www.nssn.org`).

[48] You might wonder why the acronym is not IOS for the International Organization for Standardization. Being an international organization, the acronym would be different depending on which country you were in (English would be IOS, but the French acronym would be OIN, which stands for Organisation Internationale de Normalisation). The forming members of the organization agreed upon ISO, which came from the Greek word *isos*, meaning ''equal.'' This provided a globally standard acronym for the organization.

from 157 nations. In addition to the development of international standards, the ISO also is responsible for publishing an assortment of technical reports, specifications, and guides. Following is a list of some of the available ISO standards:

- **ISO/IEC 9541 –Information Technology** — Font information interchange
- **ISO 9000** — Quality management system in production environments
- **ISO 9141** — Network interconnection of computers in a vehicle
- **ISO 15930** — Portable Document Format (PDF)

The preceding is only a short example of the many standards maintained by the ISO. For further reading, visit the ISO website at `www.iso.org`.

1.3.3 International Electrotechnical Commission

The International Electrotechnical Commission (IEC) is responsible for standards that relate to electrotechnology (electronics and related technology). The strict standards developed by the IEC are used by its members as references when standardizing electrotechnical resources and contracts. Products that are manufactured to these standards can be used regardless of where in the world you live. The IEC is credited for promoting trade and technical efficiency on a global scale. This ensures that the end user can operate the IEC-supported device without having to understand the complexities that may be involved in the technology itself.

In addition to international standards, the IEC also produces various publications that outline specifications and guidelines for areas that may not be considered standards. Many of these publications are revisions to existing standards or draft standards that are under review.

1.3.4 Telecommunications Industry Association

The Telecommunications Industry Association (TIA) develops standards that apply to telecommunications technologies. TIA has over 70 formulation groups, each of which manages different subcommittees composed of industry professionals, manufacturers, service providers, and even government representatives.

These subcommittees and formulation groups devise and develop standards that are submitted to ANSI for accreditation. TIA committees

RANDOM BONUS DEFINITION

birds of a feather (BoF) — A BoF is an informal discussion group that consists of members who share a common interest or concern.

write and maintain standards and specifications for the telecommunications industry. TIA also participates within various international telecommunications groups representing the interests of the United States on a global forum.

1.3.5 Electronic Industries Alliance

The Electronic Industries Alliance (EIA) is an association made up of technical and electronic manufacturers from the United States that cooperatively work with each other to ensure that the development and competitiveness of these companies are represented on a global scale. The issues the EIA addresses are of interest to the common good of these companies as a whole, ensuring that the companies are able to achieve the success they deserve. The EIA focuses on the following areas:

- Cyber security
- The environment
- Information technology reform
- Telecommunications reform
- Global competitiveness
- Global trade and market access

1.3.6 International Telecommunication Union

Dedicated to bringing worldwide communication to everyone, the International Telecommunication Union (ITU) is an organization that works to facilitate telecommunications and data network development and continued growth on a global scale. The ITU is striving to enable individuals everywhere to have access to benefits that are available with the information community and the global economy.

In 2007, the ITU launched the Global Cybersecurity Agenda (GCA), envisioning the future assurance of cybersecurity as well as cyber peace throughout the Internet. Another goal of the ITU is to strengthen communications to assist in disaster recovery and prevention efforts in major countries as well as developing countries that lack resources and economies to support the Information Age.

ACRONYM ALERT

RIP — Routing Information Protocol

1.3.7 IEEE

Originally, IEEE was the acronym for the Institute of Electrical and Electronics Engineers. Over time, the scope and mission of the IEEE grew into other related fields, and now the name of the organization is simply IEEE (that's I-triple-E). The IEEE develops[49] global standards applicable to information technology, telecommunications, power generation, and other related services. The IEEE has developed and maintains more than 900 standards that are active and in use. Additionally, more than 400 draft standards are in development.

The IEEE membership is made up of scientists, engineers, and other leaders in the fields of computer science, electronics, engineering, and related professions. Membership in the IEEE provides access to the latest developments in technology, assists in career development, provides access to technical information, and many other benefits.

In additional to the standards that are developed and maintained by the IEEE, the organization publishes almost a third of the world's technical literature for the fields of computer science, electrical engineering, and electronics. They also maintain an online digital library, sponsor conferences, offer educational and special-purpose grants, and bestow recognition awards.

One of the largest family of standards maintained by the IEEE is IEEE 802. The IEEE 802 organization is made up of 22 working groups (see Section 1.3.7.1) that work to develop standards applicable to LAN, MAN, and some WAN technologies. This section introduces some of the IEEE LAN standards. For more information about the IEEE, go to their website, `www.ieee.org`.

1.3.7.1 IEEE 802 Working Groups

A *working group* is a team of professionals who are brought together to work on new research activities. Usually these are formed when an individual or a group presents a suggestion for a resolution to a current standard or on the behalf of a new technology that is being mainstreamed. Working groups are often referred to as a task force, task group, study group, advisory group, and many others. Following is a list of IEEE 802 working groups and their current status:

- **Active groups**
  - 802.1 Higher Layer LAN Protocols Working Group
  - 802.3 Ethernet Working Group
  - 802.11 Wireless LAN Working Group

[49] As a matter of fact, at the time of this writing, IEEE touted that they were the leading developer of international standards.

  - 802.15 Wireless Personal Area Network (WPAN) Working Group
  - 802.16 Broadband Wireless Access Working Group
  - 802.17 Resilient Packet Ring Working Group
  - 802.18 Radio Regulatory Technical Advisory Group
  - 802.19 Coexistence Technical Advisory Group
  - 802.20 Mobile Broadband Wireless Access (MBWA) Working Group
  - 802.21 Media Independent Handoff Working Group
  - 802.22 Wireless Regional Area Networks
- **Inactive groups**[50]
  - 802.2 Logical Link Control Working Group
  - 802.5 Token Ring Working Group
- **Disbanded groups**
  - 802.4 Token Bus Working Group
  - 802.6 Metropolitan Area Network Working Group
  - 802.7 Broadband TAG
  - 802.8 Fiber Optic TAG
  - 802.9 Integrated Services LAN Working Group
  - 802.10 Security Working Group
  - 802.12 Demand Priority Working Group
  - 802.14 Cable Modem Working Group
  - QOS/FC Executive Committee Study Group

The remainder of this section lists some of the standards that have been developed by the IEEE working groups that deal with subject matter common in most LANs and MANs.[51] These working groups are IEEE 802.1, IEEE 802.3, IEEE 802.5, and IEEE 802.11.

1.3.7.2 IEEE 802.1

IEEE 802.1 is responsible for the development of numerous standards, as well as providing recommendations for the following areas: 802 LAN architecture, 802

[50] ''Inactive'' does not mean the technology is not out there; it just means there are no updates being worked on at this time.

[51] These are also the main working groups within the IEEE 802 family that sets standards for the material covered in this book.

MAN architecture, 802 WAN architecture, 802 overall network management, protocol layers above the MAC and LLC sublayers (see Section 1.4), and 802 Security. Following is a list of IEEE 802.1 standards:

- **IEEE 802.1AB** — This standard defines how to use the Link Layer Discovery Protocol (LLDP) as well as identifying node access points for network and device management.
- **IEEE 802.1AD** — This standard sets the rules used by service providers to use bridges, so they can basically provide the equivalent of a separate catenet to their customers.
- **IEEE 802.1AE** — This standard defines the MAC security guidelines for the purpose of data security.
- **IEEE 802.1B** — This standard defines the rules for remote management of IEEE 802 LANs.[52]
- **IEEE 802.1D** — Of all the 802.1 standards, this is the one that is the most well known. It is also the most used standard and outlines the rules followed by LAN bridges and switches.
- **IEEE 802.1E** — This standard outlines the rules for using multicast to reliably transfer large amounts of data to multiple network nodes.
- **IEEE 802.1F**[53] — This standard outlines some common definitions used for system management information common through the series of IEEE 802 standards.
- **IEEE 802.1G** — This standard outlines the rules that allow bridges in LANs to communication using WAN technology.
- **IEEE 802.1H** — This is more of a recommendation than a standard. It provides a way for end stations and bridges in an Ethernet LAN to communicate with end stations and bridges in other LANs that use a non-native encapsulation type.
- **IEEE 802.1Q** — This standard outlines the requirements and rules for nodes operating in an virtual LAN (VLAN). Like the 802.1D standard, this is one of the more widely used and implemented 802.1 standards.
- **IEEE 802.1X** — This standard outlines the rules that allow a way of authenticating devices attached to a LAN port at the Data Link layer (see Section 1.4).

[52] The Simple Network Management Protocol (SNMP) is the de facto standard, used by pretty much everyone. Because of this, the IEEE 802.1B standard is not used very often.

[53] SNMP has pretty much taken over. 802.1F has joined 802.1B on the not used often list.

1.3.7.3 IEEE 802.3

IEEE 802.3 is the standard for Ethernet-based LANs. It defines the rules for the Media Access Control (MAC) sublayer and the Physical sublayer of the Data Link layer (Layer 2 of the OSI reference model, which is discussed in Section 1.4) in an Ethernet LAN. IEEE 802.3 is one document maintained by the IEEE 802.3 working group — the IEEE 802.3 standard. Supplements to the standards are identified by letter designations at the end (for instance, 802.3a, 802.3c, etc.). The following is a list of some of the supplements that have been part of the 802.3 standard:

- **IEEE 802.3a** — Thin coaxial cable, 10BASE2
- **IEEE 802.3c** — Specifications for repeaters
- **IEEE 802.3d** — Fiber optic inter-repeater link
- **IEEE 802.3i** — UTP cable, 10BASE-T
- **IEEE 802.3j** — Fiber optic LAN, 10BASE-F
- **IEEE 802.3u** — Fast Ethernet, 100BASE-T
- **IEEE 802.3x** — Full duplex operation and flow control
- **IEEE 802.3z** — Gigabit Ethernet over optical fiber
- **IEEE 802.3ab** — Gigabit Ethernet over UTP cable, 1000BASE-T
- **IEEE 802.3ac** — Frame extensions for VLAN-tagging
- **IEEE 802.3ad** — Link aggregation
- **IEEE 802.3ae** — 10 Gbit/s Ethernet over fiber
- **IEEE 802.3af** — Power over Ethernet
- **IEEE 802.3ah** — Ethernet in the First Mile
- **IEEE 802.3ak** — Ethernet over Twinaxial
- **IEEE 802.3an** — 10GBASE-T
- **IEEE 802.3ap** — Backplane Ethernet
- **IEEE 802.3aq** — 10GBASE-LRM
- **IEEE 802.3as** — Frame expansion

1.3.7.4 IEEE 802.5

IEEE 802.5 is the standard for Token Ring–based LANs. I t defines the rules for the Media Access Control (MAC) sublayer and the physical sublayer of the Data Link layer (Layer 2 of the OSI reference model, which is discussed in Section 1.4) in an Token Ring LAN. IEEE 802.5 is one document that was maintained by the IEEE 802.5 working group (now inactive) — the IEEE 802.5 standard. Supplements to the standards are identified by letter designations at the end (for instance, 802.5c, 802.5j, etc.). The following is a list of some of the supplements that have been part of the 802.5 standard:

- **IEEE 802.5c** — Dual-ring redundant configuration
- **IEEE 802.5j** — Optical fiber media
- **IEEE 802.5r** — Dedicated Token Ring/full duplex operation
- **IEEE 802.5t** — 100 Mb/s High Speed Token Ring
- **IEEE 802.5v** — Gigabit Token Ring

1.3.7.5 IEEE 802.11

IEEE 802.11 is the standard for wireless LAN technology. All the supplements to 802.11 follow the basic protocol, with the difference being the frequency, speed, and distance supported. The original 802.11 standard supported an operating frequency of 2.4 Ghz.[54] The maximum supported data rate is 2 Mbit/s, with an indoor range of 20 meters and an outdoor range of 100 meters.[55]

- **IEEE 802.11a** — The 802.11a standard supports an operating frequency of 5 GHz. The maximum data rate for 802.11a is 54 Mbit/s and the average data rate is approximately 23 Mbit/s. 802.11a reaches a maximum indoor range of 35 meters and an outdoor range of 120 meters.
- **IEEE 802.11b** — The 802.11b standard supports an operating frequency of 2.4 GHz. The maximum data rate for 802.11b is 11 Mbit/s. 802.11b reaches a maximum indoor range of 38 meters and an outdoor range of 140 meters.
- **IEEE 802.11g** — The 802.11g standard supports an operating frequency of 2.4 GHz. The maximum data rate for 802.11g is 54 Mbit/s. 802.11g reaches a maximum indoor range of 38 meters and an outdoor range of 140 meters.
- **IEEE 802.11n** — The 802.11n standard supports an operating frequency of 2.4GHz and 5 GHz. The maximum data rate for 802.11n is 248 Mbit/s. 802.11n reaches a maximum indoor range of 70 meters and an outdoor range of 250 meters.

[54] In this section, operating frequencies are listed in accordance with the industrial, scientific, and medical (ISM) radio bands.

[55] Any guesses on why the outdoor range is higher? Two words: NO WALLS.

- **IEEE 802.11y** — The 802.11y standard supports an operating frequency of 3.7 GHz. The maximum data rate for 802.11y is 54 Mbit/s. 802.11y reaches a maximum indoor range of 50 meters and an outdoor range of 5000 meters.

1.3.8 Internet Society (ISOC)

The Internet Society (ISOC) was formed in 1992 as an organization dedicated to structuring the development process of Internet standards. ISOC maintains a global focus, striving to ensure that the ongoing development and growth of the Internet provides benefits to users all over the world.

ISOC has more than 27,000 members split into groups and chapters throughout the world. The main offices are in Washington, D.C., and Geneva, Switzerland. ISOC has several organizations that assist in its purpose, including the Internet Architecture Board (IAB), the Internet Research Task Force (IRTF), and others. There are three main goals that ISOC works to achieve. They support the Internet Engineering Task Force (IETF) in standards development. They also work with organizations, institutions, and other groups to form public policy to promote global equality for all global users of the Internet. Finally, ISOC is dedicated to technical education by providing training, educational grants for experts in the field in developing countries, and conferences pertaining to issues that affect the Internet.

More information can be found on the ISOC website: `www.isoc.org`.

1.3.9 Internet Engineering Task Force

The Internet Engineering Task Force (IETF) develops and maintains the standards pertaining to the TCP/IP protocol suite. Membership is open to anyone, and the committees are composed solely of volunteers (although sometimes employers and sponsors may fund research). The IETF is a task force within ISOC.

RANDOM BONUS DEFINITION

IP address — An address assigned to network nodes in order to transmit data at the Network layer.

The IETF has both working groups and birds of a feather (BoF) discussion groups. Regardless of the group type, each has a charter that explains the goals of the group. Decisions are determined by an open consensus, rather than a vote. Once a BoF or working group completes its goals, the group dissolves[56]

[56] Some working groups have it written into their charter that the working group can continue to take on new tasks that pertain to the working group.

and the members usually go on to other tasks. Following are some important terms that pertain to the standards process within the IETF:

- **Internet Architecture Board (IAB) —** The IAB is a committee within the IETF. It is responsible for defining and managing the rules for the Internet's architecture. As an IETF committee, the IAB provides oversight and direction to the IETF and is an advisory group for the ISOC.
- **Internet Assigned Numbers Authority (IANA)** — The IANA is responsible for three very important Internet technical functions. The first function is the assignment of protocol name and number registers for many Internet protocols. The second function is maintaining the top-level domain names (a.k.a. the *DNS root*), the .int domain, the .ARPA domain, as well as maintaining the Internationalized Domain Name (IDN) registry. The third service provided by the IANA is the coordination of IP addresses and Autonomous System (AS) numbering used for routing data on the Internet.
- **Internet Engineering Steering Group (IESG) —** The IESG manages the activities of the IETF and is also responsible for reviewing and monitoring Internet standards development and, ultimately, the approval of the standards.
- **Internet-Drafts** — Internet-Drafts are documents that are being worked on by the IETF or one of its working groups, BoFs, members, etc. Internet-Drafts are not approved standards and should not be treated as such. An Internet-Draft must have some revision or edit every six months, or it must be either removed or transformed into an approved standard. An Internet-Draft is also referred to as a *draft standard* (DS).
- **Request for Comments (RFCs)** — RFCs are documents that provide new technology information, updates to standards, better ways of doing things, R and D, and other miscellaneous information[57] dealing with network technologies. The IETF reviews RFCs and takes up some of ideas and proposals in the RFCs as an Internet standard. Some people confuse RFCs with Internet standards, but they are not the same thing. If the IETF decides to adopt an RFC for consideration to be a standard, it starts the RFC on a *standards track*. Initially, the RFC will be a proposed standard (PS). If the RFC makes it past the approval process, it then becomes a draft standard (DS). Finally, if the RFC gets approval through the draft process, it becomes an Internet standard (STD).

[57] You can even find some funny RFCs, such as RFC 1438, ''Internet Engineering Task Force Statements Of Boredom (SOBs), or RFC 1097, ''TELNET Subliminal-Message Option.'' There are quite a few out there; see how many you can find. Read a couple and then write to Jim or Rich and tell them which one is your favorite. Or better yet, write your own and submit it. See if it gets published.

Interested in reading more? You can get more information about the IETF on the IETF website (`www.ietf.org`).

1.4 An Introduction to the OSI Reference Model

In 1977, ANSI began work on what eventually became known as the OSI reference model.[58] A working group was formed, and the proposal was submitted to the ISO to begin working on a networking suite to develop a layer model for network architecture in an attempt to standardize. ISO and the International Telecommunication Union –Telecommunication Standardization Sector (ITU-T) participated in a joint effort to standardize networking. The joint effort became known as the Open Systems Interconnection (OSI). OSI was an effort to establish some commonality among communication protocols. Through the efforts of the OSI, the OSI protocol suite and the OSI reference model were born.

Since its inception, the OSI reference model has been the model that most networking professionals first learn about.[59] It still remains an excellent model to learn networking architecture from. It's important to note that the reference model is only a guide and not the rules for networking. It serves as a tool for vendors to follow if they want their product to be available for use in multivendor environments. It is important to note that many of the protocols on the market today are modeled after the TCP/IP reference model (see Section 1.6), and may not fit into any particular layer of the OSI reference model.

RANDOM BONUS DEFINITION

MAC address — The physical (hardware or adaptor) address that identifies a network node

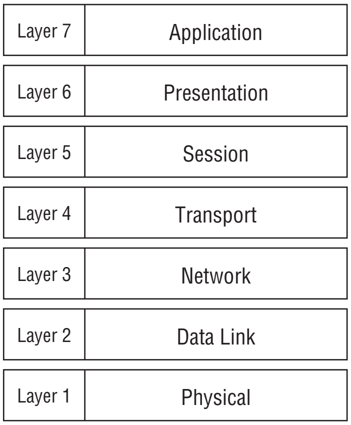
The OSI reference model is a standard reference model for data communication between network nodes. From a user's perspective, it is used as a reference to define and understand a network. From a vendor's perspective, it is used when developing a product that you expect to be able to operate with products from other vendors.

The OSI reference model divides data communication into seven layers, as shown in Figure 1-12. The lower three layers are used to pass data between

[58] The OSI reference model is also known as the OSI Basic Reference Model, the seven-layer model, and the OSI model. For the purposes of standardization, we will refer to this as the OSI reference model throughout this book. This does not infer that the other names are not appropriate, only that it is preferred by the authors.

[59] The OSI reference model has been largely superseded by publications that have been developed since it first came out.

network nodes, whereas the upper four layers are used when user data is passed between end users.



Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

Figure 1-12 The OSI reference model

1.4.1 All People Seem to Need Data Processing— A Mnemonic Device

You might think that this is silly, but no self-respecting self-teaching guide would hold back from sharing information that might be of a benefit to the reader. You need to know the layers of the reference model and what each layer does. It will not only make you sound like you know what you're doing, it will also help you understand what others are talking about. It is also about an 80 percent certainty that you are going to be asked to name the layers, so here is a quick tip on how you can remember them. Simply take the first letter of each name in the model, in order, and replace it with a word that fits into a sentence. For instance:

Application–**P**resentation–**S**ession–**T**ransport–**N**etwork–**D**ata link–**P**hysical

becomes

All–**P**eople–**S**eem–**T**o–**N**eed–**D**ata–**P**rocessing

You can also do this in reverse order:

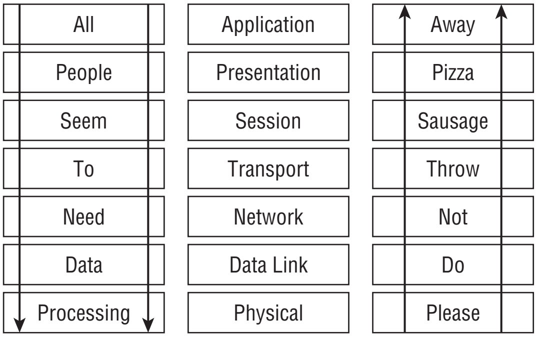
Physical–**D**ata link–**N**etwork–**T**ransport–**S**ession–**P**resentation–**A**pplication becomes

Please–**D**o–**N**ot–**T**hrow–**S**ausage–**P**izza–**A**way[60]

Figure 1-13 has an example of these two mnemonic devices, set next to the layers in the OSI model. Many other mnemonic devices have been made up for the purposes of memorizing the layers, and you're certainly welcome to create your own. Hey, if it works, don't knock it!

ACRONYM ALERT

OSPF — Open Shortest Path First



All	Application	Away
People	Presentation	Pizza
Seem	Session	Sausage
To	Transport	Throw
Need	Network	Not
Data	Data Link	Do
Processing	Physical	Please

Figure 1-13 Using a mnemonic device as a memory aid

1.4.2 A Layered Approach

The OSI reference model is a systematic approach to outlining the services of protocols that define network architecture. Each layer within the model works with the layers above and/or below them to serve a data transmission purpose. In most networks, the theory of the OSI model may not represent the entire network, and that is why it is a reference model, not a required set of rules.

The OSI reference model breaks down the services within a network into seven layers. Each layer represents protocols that perform a certain purpose or method for allowing data communication within the network. Data is transmitted from a user on the network to another user. It is an application that begins and ends the network connection process. As shown in Figure 1-14,

[60] Jim actually once interviewed an individual who when asked to name the layers of the OSI model actually said, ''Please do not throw sausage pizza away'' out loud to remember the layer names. His intention wasn't to say it out loud, but he did. He also ended up getting the job.

data flows from Layer 7 to Layer 1, is transmitted to the destination, where it travels up the layers to the end user. So what exactly is going on in these layers? Let's talk about that for a while.

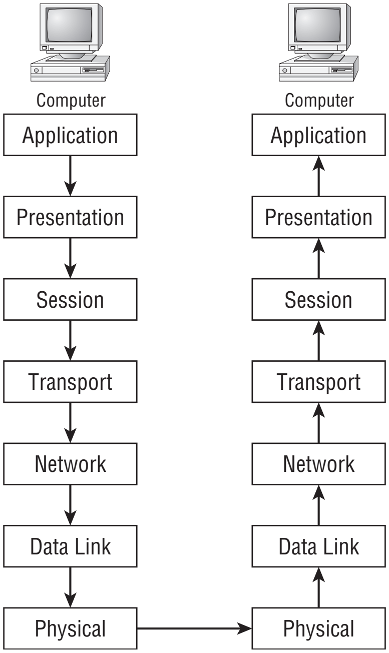


Figure 1-14 A complete, end-to-end network connection

1.4.2.1 Layer 7 — The Application Layer

The name *application* might confuse you at first. The Application layer contains the operating systems that enable application programs to interface with the network. This layer serves application processes that the network uses, but not the applications that interface with the user. Let's look at a couple of examples.

- **Example 1: Sending an e-mail** — The Application layer defines the protocols used in an e-mail transmission, but not the interface that the end user has to initiate in order to send the e-mail.
- **Example 2: Initiating an FTP session** — The Application layer defines the protocol used for a file transfer, but the end user has to initiate an interface with an FTP application to perform the file transfer.

Keep in mind that the OSI reference model is for the architecture of networks and network nodes. Therefore, the Presentation layer does not define end users and the interfaces they have with a PC (and the applications running on the

PC). Not only does the Application layer serve the applications process, it also sends service requests to the Presentation layer. Examples of some common, and a few uncommon, Application layer protocols and services include:

- Association Control Service Element (ACSE)
- Common Management Information Protocol (CMIP)
- Common Management Information Service (CMIS)
- CMIP over TCP/IP (CMOT)
- Dynamic Host Configuration Protocol (DHCP)
- File Transfer Access and Management (FTAM)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Internet Relay Chat (IRC)
- Network File System (NFS)
- Post Office Protocol 3 (POP3)
- Remote Operation Service Element (ROSE)
- Reliable Transfer Service Element (RTSE)
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
- Telecommunications Network (Telnet)
- Virtual Terminal Protocol (VSP)
- X.400 –Message Handling Service Protocols
- X.500 –Directory Access Service Protocol (DAP)

1.4.2.2 Layer 6 — The Presentation Layer

The Presentation layer responds to service requests from the Application layer, and sends service requests to the Session layer. The Presentation layer also is responsible for accepting data from the lower layers and then presenting the data to the Application layer, and, ultimately, to the destination. The following functions operate at the Presentation layer:

- Encryption services
- Decryption services
- Data compression services
- Data decompression services
- Translation services

The Presentation layer takes care of translating data from lower layers so the data is understood at the Application layer. This saves the Application layer the headache of having to translate the data itself. The translation also occurs at the Presentation layer when data is being passed down the stack from the Application layer. Note that the Presentation layer is not always needed[61] and that the Application layer may actually work with the Session layer and keep the Presentation layer out of the loop. Here are some examples of the data formats that are defined at the Presentation layer:

- American Standard Code for Information Interchange (ASCII)
- Binary
- Extended Binary Coded Decimal Interchange Code (EBCDIC)
- Joint Photographic Experts Group (JPEG)
- Musical Instrument Digital Interface (MIDI)

1.4.2.3 Layer 5 — The Session Layer

The Session layer is responsible for setting up communication between nodes. The Session layer responds to service requests from the Presentation layer[62] as well as sending service requests to the Transport layer. The Session layer may also provide access control services, authentication, data synchronization, and other services.

The Session layer establishes a communication session, manages the session, and then terminates the session between endpoints. The Session layer is able to gather data streams that are coming from multiple originators and can ensure that the data is synchronized correctly for the destination.[63]

Here are some examples of the data formats defined at the Session layer:

- Network Basic Input/Output System (NetBIOS)
- Network File System (NFS)
- Secure Shell (SSH)
- Structured Query Language (SQL)

1.4.2.4 Layer 4 — The Transport Layer

The Transport layer takes care of getting data from endpoint to endpoint. As long as there is an open communications path, the Transport layer can do its job. The Transport layer receives requests from the Session layer and sends

[61] This is due to the fact that encryption/decryption and compression/decompression are not always used.

[62] As mentioned previously, the session layer can also respond to the application layer if the presentation layer is not necessary for a session.

[63] Imagine how much fun we would all have if the destination had to just figure it out on its own.

requests on to the Network layer. The Transport layer ensures end-to-end delivery of data, allowing communication to occur between various endpoint nodes within a network.

The Transport layer utilizes various standards to ensure that data arrives in the right order and that its integrity is maintained. To do this, several functions occur at the Transport layer, including:

- Ensuring that a connection is established
- Disassembling and then reassembling large data streams
- Flow control
- Error recovery
- Data sequencing

The Transport layer is similar to a delivery service, such as the U.S. Postal Service, UPS, or Fed-Ex. They sort, separate, and distribute packages, and have different priorities and classifications. Without caring what is in the package, they get the package where it is supposed to go.[64]

Some examples of Transport layer protocols include:

- AppleTalk Transaction Protocol (ATP)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Sequenced Packet Exchange (SPX)

1.4.2.5 Layer 3 — The Network Layer

The Network layer is responsible for exchanging data between nodes across several data paths. The Network layer uses nodes called routers to route packets from endpoint to endpoint. The Network layer allows the packet to pass through various network topologies, choosing from multiple paths until it reaches its destination.

The Network layer is able to transfer variable amounts of data between endpoints over one or more networks. The Network layer breaks data into smaller packets and then reassembles the data once it arrives at its destination. The Network layer is also responsible for identifying when an error in data transmission occurs.

IP is the most well-known and widely used Network layer protocol. Remember, IP is connectionless and is not required to regulate and ensure reliable data delivery. It does, however, identify errors in transmission, ensuring that bad packets are dropped. Also, it is IP that fragments data into packets that the next node on the network can support.

[64] Hopefully in the condition it is expected to arrive in.

Some examples of Network layer protocols include:

- Internet Protocol (IP)
- Internetwork Packet Exchange protocol (IPX)
- Routing Information Protocol (RIP)
- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Open Shortest Path First (OSPF)
- Internet Group Management Protocol (IGMP)

1.4.2.6 Layer 2 — The Data Link Layer

For the most part, LAN communication is handled at the Data Link layer and the Physical layer. At the Data Link layer, network nodes known as *switches* or *bridges* pass frames between nodes in the LAN. Data communication at the Data Link layer can be between two nodes (point-to-point) or between a single endpoint node to many endpoint nodes (point-to-multipoint).

The Data Link layer ensures data delivery between nodes, using the physical addresses of the nodes. It is important that considerations are made for the physical topology of the network segment for the data link traffic. The Data Link layer provides for data flow control, which is used to prevent a node from receiving more data than it can handle at any particular time. The Data Link layer also provides for error notification to the upper layers when a data transmission error occurs.

RANDOM BONUS DEFINITION

multiplexing — The act of combining multiple data streams into a single signal and then transmitting the data over a shared medium. Also known as *muxing*.

Some examples of Data Link layer protocols include:

- High-level Data Link Control (HDLC)
- Serial Line Internet Protocol (SLIP)
- Point-to-Point Protocol (PPP)

The IEEE divides the Data Link layer into two sublayers: the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer. The LLC sublayer is referred to as the *upper sublayer* of the Data Link layer, whereas the MAC sublayer is the *lower sublayer*. The LLC sublayer multiplexes and demultiplexes data transmitted over the MAC sublayer. The IEEE standard that encompasses the LLC sublayer is IEEE 802.2. The MAC sublayer acts as an interface between the LLC sublayer and the Physical layer. The MAC sublayer makes it possible for network nodes to communication within a multipoint network (such as a LAN or a MAN), by providing address and access control services.

1.4.2.7 Layer 1 — The Physical Layer

The Physical layer serves the Data Link layer. The Physical layer provides a way for the data to be transmitted in a network. Data is converted into a signal which is passed to an endpoint over a physical connection. The Physical layer is responsible for the procedures, mechanics, and the electricity required for operating.

Examples of network nodes that are Physical layer nodes include network adaptors (NIC cards), network hubs, and modems.

1.5 TCP/IP, Please (and Don't Be Stingy with the IP)

TCP/IP is the main protocol used by the Internet and most other network types. If you are a node that connects directly to the Internet, then you will use the TCP/IP protocol to communicate with other nodes. Earlier you learned that TCP and IP are two separate protocols that work with one another. TCP handles breaking down data into small packages, known as *packets*, and then puts the data back together when the data arrives at its destination. IP knows how to get the data there. In this section, we introduce TCP/IP. In Chapter 2, ‘‘The TCP/IP Protocol Suite,’’ we will discuss it more in depth. This introduction is required, however, because you will need to have a basic understanding for some of the material covered in Chapters 2 through 4.

A network is simply nodes that are connected to one another to pass data. For data to arrive intact and at the right destination, you must have the protocols that can make sure this happens. This combination of protocols is the TCP/IP protocol suite. TCP/IP was brought about to standardize communications protocols, as there were a lot of proprietary protocols when networking was in its infancy.

POP QUIZ

What is ARPANET? (Note: If you don't know the answer to this one, go back and reread Section 1.2. The next paragraph is where that information starts to come in handy.)

POP QUIZ

Name the four IMPs that made up the original ARPANET.

If you are reading this, that means you remember what ARPANET was. This is important, because you probably remember when those supercomputers from different geographical areas first talked to each other. Well, the ARPANET protocols that made that happen are what is now known as TCP/IP. The name TCP/IP somewhat implies that these two protocols are what makes TCP/IP what it is. Actually, TCP/IP is a collection of several protocols that work with one another to accomplish data transmission. TCP/IP has its own reference model (see Section 1.5.3) that basically follows the OSI reference model. The protocols that make up TCP/IP use the TCP/IP reference model to map out where they are to function.

Over the years, other protocols have been used to provide upper-layer functionality to transmit data. There are still a few of these out there, but most people support and utilize the TCP/IP protocol. Why use TCP/IP? The answer is simple: because everyone uses TCP/IP. Besides the fact that everyone uses it in some fashion or another, there are several other reasons why TCP/IP has grown into the ''method of choice.'' Some of these are:

- **Routing** — TCP/IP was designed to route data from node to node of networks of variable sizes and complexities. TCP/IP is not worried about the status of nodes in the network; it is concerned about the networks that it should know about. Various protocols within the TCP/IP protocol suite manage data flow between networks.
- **Addressing** — And guess what is built into TCP/IP? That's right, IP. IP provides a way for a node to identify other nodes within a network and deliver data to any endpoint node it has been made aware of.
- **Name resolution** — TCP/IP provides a way to map an IP address (10.10.10.10) to an actual name (`networkz.org`). Can you imagine how tough it would be to remember the IP addresses of all the websites you needed to know about? Name resolution really helps.
- **Doesn't discount the lower layers** — Although TCP/IP operates at the upper layers (Layer 3 and above), it does have the ability to operate at the lower levels as well. This means that for most LANs and WLANs, and some MANs and WANs, TCP/IP is able to work with multiple networks of these types and connect them to each other.
- **Open standards** — TCP/IP was mainstreamed to enable different nodes to communicate with one another. The open standards that TCP/IP contains are available to anyone. These standards are determined through the RFC process discussed in Section 1.3.9.

- **Talking endpoint to endpoint** — TCP/IP provides a way for one endpoint to speak directly with another endpoint, regardless of any nodes that are in between. It is as if the endpoints were directly connected to one another, even when they are not physically connected to the same local network. Thanks to TCP/IP, both the originating and the destination nodes can exchange connection acknowledgements directly with one another.
- **Application support** — TCP/IP provides protocols that provide a commonality among end user applications. Often when an application that utilizes TCP/IP is developed, many of the functions required for the application are already common with any node supporting TCP/IP.

There are some basic Network layer services provided by any network. All user applications that utilize TCP/IP rely on these standard services to assist in data transport. The first of these standards is that TCP/IP supports connectionless datagram delivery. The TCP/IP network is able to route data from node to node based on the address of the source and destination nodes, but is not concerned about the order in which the data is sent. Having connectionless datagram delivery gives TCP/IP the flexibility to support a wide range of hardware through the network. The other basic service that is used by TCP/IP applications is a reliable transport service. Endpoints establish a connection prior to exchanging data. This allows a temporary connection to appear, from a user's perspective, as a direct connection. The connection remains while the endpoints exchange data (regardless of the amount of data that is transported).

1.5.1 TCP/IP Applications

End users are able to navigate networks by using applications based on the TCP/IP protocol suite. They are able to do so without having any understanding of exactly what it takes to get information shared with destination nodes. The only details the average user needs to know is how the actual interface works. Users rely on the software and technology to get the data to an endpoint.

Numerous TCP/IP-based applications are in deployment within networks worldwide. The following list contains some of the more popular applications that are widely used today:

- Electronic mail (e-mail)
- File transfer
- IP address allocation
- Remote login
- Web browser

1.5.2 TCP/IP Utilities

In addition to application support, TCP/IP also provides some helpful utilities that are available in any node that supports TCP/IP. These utilities provide a variety of information that can be used to help maintain the network. These utilities will be discussed in detail throughout the book. It is important to be aware of these, and no good networking introduction would be complete without a summary of the utilities and the purpose they serve. There are three main categories of TCP/IP utilities:

- **Diagnostic utilities** — These utilities assist in troubleshooting issues within the network.
- **General purpose utilities** — These utilities are used to connect to other TCP/IP nodes to perform a specific action, to exchange data, or to allow remote management and related services.
- **Services utilities** — These utilities are software applications that are offered by a TCP/IP-based server to TCP/IP clients.

Table 1-1 contains a list of some commonly used TCP/IP utilities.

Table 1-1 TCP/IP utilities

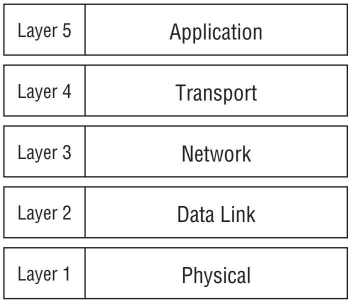
DIAGNOSTIC UTILITIES	GENERAL PURPOSE UTILITIES	SERVICES UTILITIES
Address Resolution Protocol (ARP)	File Transfer Protocol (FTP)	TCP/IP print server
IPConfig	Line Printer Daemon (LPD)	Web server
Line Printer Daemon (LPD)	Remote Copy Protocol (RCP)	File Transfer Protocol server
netstat	Remote Shell (RSH)	E-mail server
nslookup	Telnet	
ping	Trivial File Transfer Protocol (TFTP)	
route		
tracert (Windows) Traceroute (other operating systems, such as Linux, Unix, and others)		

1.5.3 The TCP/IP Reference Model

The TCP/IP reference model, the specification established by DARPA[65] to set the rules for ARPANET (and now maintained by the IETF), was developed long before the OSI reference model. Rather than the seven-layer OSI reference model, the TCP/IP reference model has only five[66] layers, as shown in Figure 1-15.

POP QUIZ

What is the Post Office Protocol?



Layer 5	Application
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

Figure 1-15 The TCP/IP reference model

An important thing to note is that the TCP/IP reference model, although represented in layers, does not really operate in a layered manner as the OSI reference model does. There is not a lot of agreement where the layers really fall, though you will often hear about the upper and lower layers in the TCP/IP reference model. The main point is that regardless of whether you follow the OSI reference model or the TCP/IP reference model, the functionality of the network is, for the most part, the same.

As mentioned previously, Chapter 2 discusses the TCP/IP reference model in depth. For the purposes of this introductory chapter, it is important to have only an introduction to the model. The TCP/IP reference model layers are:

- **Application layer (Layer 5)** — The Application layer in the TCP/IP reference model assumes most of the functions performed by the Session and Presentation layers of the OSI reference model. All upper-layer protocols are handled at this layer.

[65] At least we think it was DARPA . . . or was it ARPA? Okay, enough funning around — it was DARPA at the time.

[66] A lot of people don't consider the physical layer to be part of the TCP/IP reference model. For the purposes of this book, we have decided to include the physical layer. We don't want you to be confused in the future when someone mentions the four-layer TCP/IP model.

- **Transport layer (Layer 4)** — The Transport layer functions the same in both reference models. The two major protocols that operate at this layer are TCP and UDP. TCP is a connection-oriented protocol and therefore provides reliable delivery. UDP, on the other hand, is connectionless and provides unreliable data delivery.
- **Network layer or Internet layer (Layer 3)** — This layer performs the same functions as Layer 3 of the OSI reference model. The network layer is responsible for routing a packet from a source to a destination. It can do this within a LAN as well as over multiple LANs, MANs, and WANs.
- **Data Link layer (Layer 2**) — This layer is often combined with the Physical layer and is referred to as the host to Network layer. The TCP/IP reference model largely ignores these lower layers. All it cares about it that there is a connection to pass data on.
- **Physical layer (Layer 1)** — This layer is often combined with the Data Link layer and is largely ignored as well, although it does provide the connections to get data passed to a destination. Make no mistake, however: If the Physical layer isn't working, you will miss it real quick. It's like that old saying, ''You don't know what you've got until it's gone.''

1.6 Chapter Exercises

1. The network used exclusively by the University of Texas is an example of a ____________ area network.
2. What are the names of the layers in the OSI reference model?

   Layer 7 ________________________________

   Layer 6 ________________________________

   Layer 5 ________________________________

   Layer 4 ________________________________

   Layer 3 ________________________________

   Layer 2 ________________________________

   Layer 1 ________________________________
3. List at least five applications and/or utilities that use TCP/IP.

   ____

   ____

   ____

4. What are the two types of network relationships?

5. Explain the difference between a client/server network relationship and a client/server database system.

6. What is the 1822 protocol?

7. What are the three types of standards? Do a search on the Internet to see if you can find at least one of each standard type.

8. The 802.11n standard supports an operating frequency of ____________ and ____________. The maximum data rate for 802.11n is ____________. 802.11n reaches a maximum indoor range of 7 ____________ and an outdoor range of 250 meters.

9. T or F: The application layer of the OSI model concerns itself with the application/user interface on a PC. ____________

10. In this chapter, we listed seven reasons why TCP/IP has grown to be the method of choice. What are these seven reasons?

1.7 Pop Quiz Answers

1. What is a public key certificate?

   Public key certificates are electronic documents that can verify and authorize an individual by public key cryptography. In public key cryptography, two keys (one public key and one private key) are used to encrypt and then decrypt data to ensure that a message can be transported securely.
2. Encapsulated data that is transmitted and received at the network layer is called a *packet*.
3. What is the difference between a physical port and a TCP port?

   A *physical port* is an interface that resides on a network node. A *TCP/IP port* is a number that is in the data packet header that maps to a process running on a node.
4. Because IP does not establish a connection before sending data to an endpoint, it would be considered a *connectionless* protocol.
5. What is the difference between a WAN and a LAN?

   The main difference between a *LAN* and a *WAN* is the size of the geographical area that is covered. A *LAN* covers a small geographical area whereas a *WAN* covers a large geographical area.
6. The three types of standards are called a *de facto* standard, a *proprietary* standard, and an *open* standard.
7. What is ARPANET?

   ARPANET stands for the Advanced Research Projects Agency Network and was the first packet-switching network ever. The Internet was developed from the ARPANET.
8. Name the four IMPs that made up the original ARPANET.

   - Stanford Research Institute
   - University of California, Los Angeles

- University of California, Santa Barbara
- University of Utah

9. What is the Post Office Protocol?

   Post Office Protocol (POP) is a protocol that allows an e-mail client to connect to an e-mail server and retrieve mail that is destined for that client.