DATA COMMUNICATIONS AND COMPUTER NETWORKS

Network Protocols

Understanding the concepts of networking protocols is critical to being able to troubleshoot communication problems in networking environments. This section will introduce you to four common network protocols found in networking environments and the difference between routable and non-routable protocols.

A network protocol is a language that is used by systems that wish to communicate with one another. If two systems wish to communicate (or talk) with one another, they need to speak the same language (or protocol). Let's look at an example of a communication problem that could occur when two persons who want to talk are not speaking the same language. Let's say that you were traveling the country on your summer vacation and took a pit stop into a fast food restaurant.

When ordering your favorite meal, you would need to ensure that you spoke the same language as the person taking the order. If you speak English and the waiter speaks French, you would be giving your order, but the waiter would not be able to understand you. The same thing will happen on the network when two systems use two totally different protocols—everyone is talking but no one is communicating.

The first step to networking is making sure that the two systems that are trying to talk have the same protocol installed.

Four of the major protocols found in networking environments today are

- NetBEUI
- IPX/SPX
- AppleTalk
- TCP/IP

NetBEUI

NetBIOS Extended User Interface (NetBEUI) is a transport protocol developed by IBM but adopted by Microsoft for use in earlier versions of Windows and DOS. NetBEUI commonly was found in smaller networks due to the fact that it is a non-routable protocol. A non-routable protocol is a protocol that sends data, but the data is unable to cross a router to reach other networks; communication is limited to the local LAN only. The fact that NetBEUI is a non-routable protocol has limited the use of NetBEUI on networks today dramatically.

NetBEUI was first implemented with LAN Manager networks and became popular in smaller Microsoft networks back in the Windows 3.11, Windows 95, and Windows 98 days. NetBEUI is an extremely efficient and simple protocol with little overhead because of its inability to route packets. One of the major advantages of NetBEUI is that it is extremely simple to install and configure.

What Is NetBIOS?

NetBEUI has a close friend, NetBIOS (short for Network Basic Input/Output System), with which it works closely when communicating with systems on the network. NetBIOS is an application programming interface (API) that is used to make network calls to remote systems. When you install NetBEUI, it includes the NetBIOS protocol, and NetBEUI relies on NetBIOS for session management functionality. Also, NetBIOS is non-routable but may be installed with other routable protocols such as IPX/SPX or TCP/IP to allow NetBIOS traffic to travel across networks. NetBIOS has two communication modes:

- Session mode Is used for connection-oriented communication in whichNetBIOS would be responsible for establishing a session with the targetsystem, monitoring the session to detect any errors in transmission, and thenrecovering from those errors by retransmitting any data that went missing orwas corrupt.
- Datagram mode Is used for connectionless communication in which asession is not needed. Datagram mode also is used for any broadcast byNetBIOS.

Datagram mode does not support error detection and correctionservices, which are therefore the responsibility of the application using NetBIOS.

Here is a list of facts about
NetBIOS and NetBEUI:

- NetBIOS is a session protocol, whereas NetBEUI is a transport protocol (more on session and transport later in this chapter, when you learn about theOSI model).
- NetBIOS is used by other protocols as well, such as TCP/IP.
- Since NetBIOS is not a transport protocol, it does not directly supportrouting but depends on one of three transport protocols—TCP/IP, IPX/SPX, or NetBEUI—to do this.
- NetBIOS uses NetBIOS names as a method of identifying systems onthe network. A NetBIOS name, also known as a computer name, can bea maximum of 16 bytes long—15 bytes for the name and 1 byte for theNetBIOS name suffix (a code at the end of the name representing the

IPX/SPX
Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) is a protocol suite (which means there are many protocols in one) that was developed by Novell and was very popular on older NetWare networks. However, newer versions of NetWare (NetWare 5.x and above) have moved away from it and are using TCP/IP as the preferred protocol. Microsoft refers to IPX/SPX as NWLink (NetWare Link). The IPX protocol of the IPX/SPX protocol suite is responsible for the routing of information across the network. IPX/SPX is a routable protocol, so its addressing scheme must be able to identify each system on the network and the network it exists on. The network administrator assigns each network a network
ID. An IPX network ID is an eight-character hexadecimal value—for example, 0BADBEEF.

A complete IPX address is made up of the network ID, a period (.), and then the six-byte MAC address of the network card (a unique address burned into the network card) in the system. For example, a computer has a MAC address of 00-90-4B-4C-C1-59. If the system were connected to network ID0BADBEEF, then the IPX network address would be 0BADBEEF.00904B4CC159.

The fact that the MAC address is used in the address means that there is no need to have it resolved when communication occurs—which will make the protocol more efficient than other protocols such as TCP/IP, which does require the IP address to be resolved to a MAC address.

IPX/SPX is not as easy to configure as NetBEUI. When doing an IPX installation, you will need to be familiar with configuration issues such as the network number and frame type.

- Network number is the number assigned to the Novell network segment.It is a hexadecimal value, eight digits maximum.
- Frame type is the format of the packet that is used by the network. It isimportant to make sure that all systems on the network are configured for thesame frame type. For example, if I wish want to connect to SERVER1, whichuses the frame type of 802.2, then I would need to ensure that my frametype was set to 802.2—otherwise, I would not be able to communicate withSERVER1. The four major frame types are 802.2, 802.3, ETHERNET_SNAP,and ETHERNET_II.

The Microsoft operating systems default to an auto setting on the frame type, which allows the IPX/SPX protocol to “sense” the frame type being used on the network and configure itself for that frame type. This has made the configuration of IPX/SPX much easier during the past few years.

While IPX is responsible for the routing of packets, it is also a connectionless, unreliable transport. Unreliable means IPX packets are sent to a destination without requiring the destination to acknowledge receiving those packets. Connectionless means that no session is established between sender and receiver before transmitting data. SPX is the protocol in the IPX/SPX protocol suite that is responsible for reliable delivery. SPX is a connection-oriented protocol that will ensure that packets that are not received at the destination are retransmitted on the wire.

AppleTalk

AppleTalk is a routable protocol that is used primarily in Macintosh environments to connect multiple systems together in a network environment. AppleTalk wasimplemented in two phases, known as phase 1 and phase 2, with the second phasebeing more popular today:

- **Phase 1** was designed for small workgroup environments and thereforesupports a much smaller number of nodes on the network. Phase 1 supports non-extended networks; each network segment is allowed to be assigned onlya single network number, and only one zone is allowed in a non-extended network. A zone is a logical grouping of nodes—the network administratorwill assign nodes to a particular zone.
- **Phase 2** was designed for larger networks and supports more than 200 hosts on the network. Phase 2 supports extended networks, thereby allowing one network segment to be assigned multiple network numbers and allowing for multiple zones on that network segment. Each node is part of a singlezone on an extended network.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is the most common protocol used today. A routable protocol, TCP/IP is the protocol on which the Internet is built. TCP/IP is very robust and commonly is associated with UNIX and Linux systems.

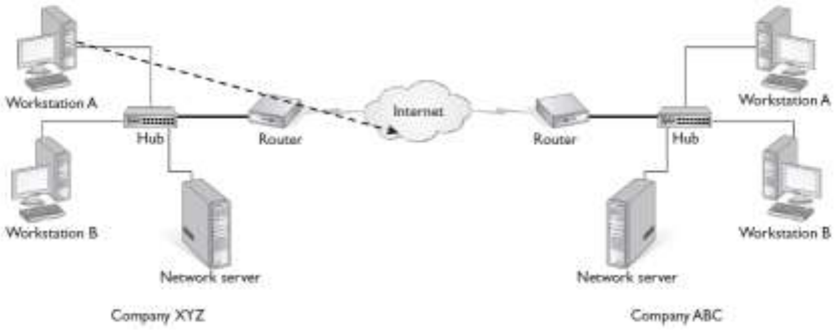
TCP/IP originally was designed in the 1970s to be used by the Defense Advanced Research Projects Agency (DARPA) and the U.S. Department of Defense (DOD) to connect dissimilar systems across the country. This design required the capability to cope with unstable network conditions. Therefore, the design of TCP/IP included the capability to reroute packets.

One of the major advantages of TCP/IP was the fact that it could be used to connect heterogeneous environments together, which is why it has become the protocol of the Internet—but what are its drawbacks? TCP/IP has two major drawbacks:

- **Configuration -** TCP/IP is a protocol that requires configuration, and to administer it, you need to be familiar with IP addresses, subnet masks, and default gateways—not complicated topics once you are familiar with them, but there is a bit of a learning curve compared to installing NetBEUI.
- **Security -** Because of the open design of TCP/IP, it has become a very insecure protocol. If security is of concern, you need to make certain that you implement additional technologies to secure the network traffic or systems running TCP/IP. For example, if you want to ensure that other individuals cannot read the data sent to your web server, you would SSL enable the web site—which would encrypttraffic between a client and your web server.

Routable vs. Non-routable Protocols

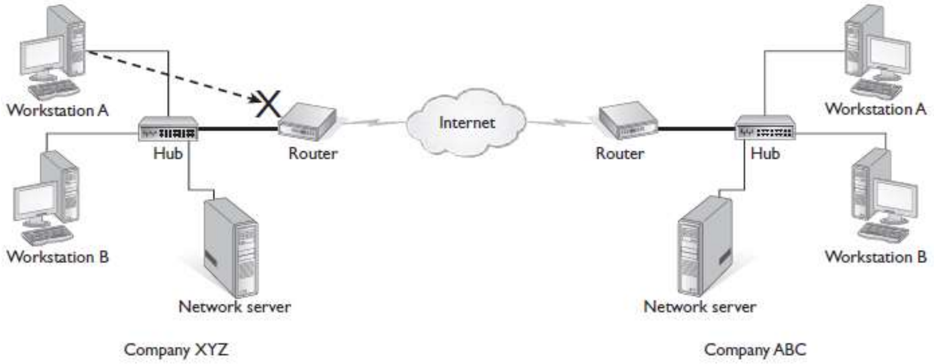
NetBEUI is a non-routable protocol, whereas IPX/SPX, AppleTalk, and TCP/IP are routable protocols. A routable protocol is a protocol whose packets may leave your network, pass through your router, and be delivered to a remote network. A non-routable protocol is a protocol that does not have the capability to cross a router to be sent from one network to another network. This is due to the fact that the protocol is designed as a simple protocol and does not accommodate addressing patterns in the packets that give knowledge of multiple networks. For example, NetBEUI uses NetBIOS names as a method to send data back and forth, but a NETBIOS name does not identify “what network” the destination system exists on, whereas TCP/IP and IPX/SPX both have a network ID portion to their addressing schemes that identify “what network” the destination system exists on.



A routable protocol sending data through a router

The OSI Model

In 1984, the International Organization for Standardization (ISO) defined astandard, or set of rules, for manufacturers of networking components that wouldallow these networking components to communicate in dissimilar environments.This standard is known as the Open Systems Interconnect (OSI) model and is a model made up of seven layers. Each layer of the OSI model is responsible for a specific function or task within the stages of network communication. Network communication starts at the application layer of the OSI model (on the sending system) and works its waydown through the layers to the physical layer. The information then passes along the communication medium to the receiving computer, which works its way backup the layers starting at the physical layer.

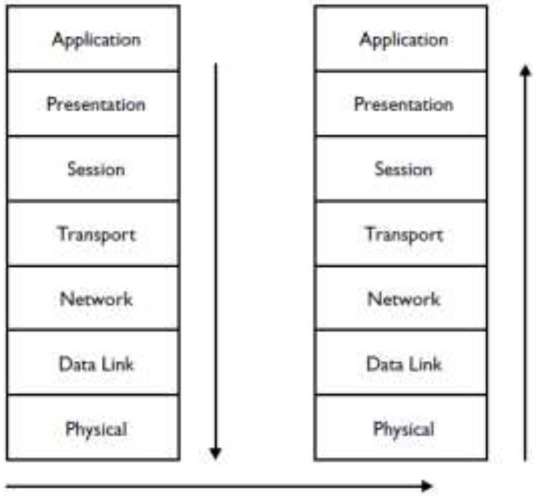


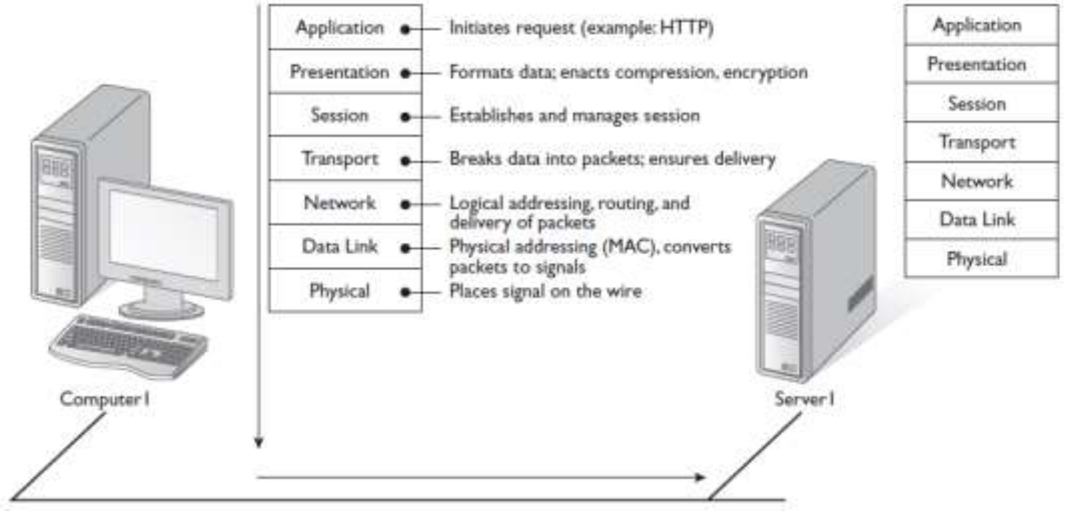
A non-routable protocol cannot send data across routers.

Each layer of the OSI model is responsible for certain functions within the process of sending data from one system to another. Each layer is responsible for communicating with the layers immediately above it and below it. For example, the presentation layer will receive information from the application layer, format it appropriately, and then pass it to the session layer. As another example, the presentation layer will never deal directly with the network or data link layers. The figures below show the OSI model.

Layer 7: The Application Layer

The application layer running on the sending system (COMPUTER1) is responsiblefor the actual request to be made. This could be any type of networking request—a web request using a web browser (HTTP), an e-mail delivery request using SMTP,or a file system request using the network client redirector software. On the receiving system, the application layer would be responsible for passing the request to the appropriate application or service on that system




Application
Initiates request (example: HTTP)
Presentation
Formats data; enacts compression, encryption
Session
Establishes and manages session
Transport
Breaks data into packets; ensures delivery
Network
Logical addressing, routing, and delivery of packets
Data Link
Physical addressing (MAC), converts packets to signals
Physical
Places signal on the wire
Application
Presentation
Session
Transport
Network
Data Link
Physical
Computer I
Server I

Layer 6: The Presentation Layer

After the request is made, the application layer passes the data down to the presentation layer, where it is to be formatted so that the data (or request) can be interpreted by the receiving system. When the presentation layer receives data from the application layer to be sent over the network, it makes sure that the data is in the proper format—if it is not, the presentation layer converts the data. On the receiving system, when the presentation layer receives network data from the session layer, it makes sure that the data is in the proper format and once again converts it if it is not.

Formatting functions that could occur at the presentation layer could be compression, encryption, and ensuring that the character code set can be interpreted on the other side.

Layer 5: The Session Layer

The session layer manages the dialog between computers. It does this by establishing, managing, and terminating communications between two computers. When a session is established, three distinct phases are involved. In the establishment phase, the requestor initiates the service and the rules for communication between the two systems. These rules could include such things as who transmits and when, as well as how much data can be sent at a time. Both systems must agree on the rules; the rules are like the etiquette of the conversation. Once the rules are established, the data transfer phase begins. Both sides know how to talk to each other, the most efficient methods to use, and how to detect errors, all because of the rules defined in the first phase. Finally, termination occurs when the session is complete, and communication ends in an orderly fashion.

Layer 4: The Transport Layer

The transport layer handles transport functions such as reliable and unreliable delivery of the data. For reliable transport protocols, the transport layer works hard to ensure reliable delivery of data to its destinations. On the sending system, the transport layer is responsible for breaking the data into smaller packets, so that if retransmission is required, only the packets missing will be sent. Missing packets are determined by the fact that the transport layer receives acknowledgments (ACKs) from the remote system, when the remote system receives the packets. At the receiving system, the transport layer will be responsible for opening all of the packets and reconstructing the original message.

Another function of the transport layer is segment sequencing. Sequencing is a connection-oriented service that takes segments that are received out of order and re-sequences them in the right order. For example, if I send you five packets and you receive the packets in this order (by their sequence number): 3, 1, 4, 2, 5, the transport layer will read the sequence numbers and assemble them in the correct order.

The transport layer also enables the option of specifying a "service address" for the services or application on the source and destination computers to specify what application the request came from and what application the request is headed for. All modern operating systems run many programs at once, and each program has a unique service address. Service addresses that are well defined (by networking standards, for example) are called well-known addresses. Service addresses also are called sockets or ports by protocols such as TCP/IP.

Layer 3: The Network Layer

The network layer is responsible for managing logical addressing information in the packets and the delivery, or routing, of those packets by using information stored in a routing table. The routing table is a list of available destinations that are stored in memory on the routers. The network layer is responsible for working with logical addresses. The logical addresses are address types that are used to uniquely identify a system on the network, but at the same time identify the network that system resides on. This is unlike a MAC address (the physical address burned into the network card), because a MAC address just gives the system a unique address and does not specify or imply what network the system lives on. The logical address is used by network-layer protocols to deliver the packets to the correct network.

Layer 2: The Data Link Layer

The data link layer is responsible for converting the data from a packet to a pattern of electrical bit signals that will be used to send the data across the communication medium. On the receiving system, the electrical signals will be converted to packets by the data link layer and then passed up to the network layer for further processing. The data link layer is divided into two sub-layers:

- **Logical link control (LLC)** is responsible for error correction and control functions.
- **Media access control (MAC)** determines the physical addressing of the hosts. It also determines how the host places traffic on the medium, for example CSMA/CD versus Token Passing.

The MAC sub-layer maintains physical device addresses (commonly referred to as MAC addresses) for communicating with other devices on the network. These physical addresses are burned into the network cards and constitute the low-level address used to determine the source and destination of network traffic.

Layer 1: The Physical Layer

The bottom layer of the OSI hierarchy is concerned only with moving bits of data onto and off the network medium. This includes the physical topology (or structure) of the network, the electrical and physical aspects of the medium used, and encoding and timing of bit transmission and reception.

Protocols and the OSI Layers

Different protocols work at different levels of the OSI model. Listed are a few of the main protocols, apply them to the OSI model, and see how they fit in the OSI model's seven layers

IPX

IPX is an extremely fast, streamlined protocol that is not connection oriented. IPX was once fairly common because of its widespread use on Novell NetWare. IPX is a routable protocol that is located at the network layer of the OSI model. Because it is also an unreliable connectionless transport, IPX also applies to layer 4—the transport layer. Remember, unreliable means data is sent without acknowledgment of receipt, and connectionless means that a session is not established before transmitting.

IPX is capable of being run over both Ethernet and Token Ring networks using the appropriate network interface card (NIC). For a number of years, IPX over Ethernet was the default use of NICs.

SPX

Sequenced Packet Exchange (SPX) is a transport protocol used by IPX for connection-oriented communication. It is responsible for breaking the message into manageable packets and ensuring the data reaches the destination. SPX is the equivalent to TCP but for the IPX/SPX protocol suite. Because SPX runs at the transport layer, it is considered a layer-4 protocol.

IP

The Internet Protocol (IP) in the TCP/IP protocol suite performs the same routing functions that IPX does for the IPX/SPX protocol suite. IP is responsible for the logical addressing and routing of messages across the network. IP does not ensure the delivery of the packets; that is the responsibility of higher-layer protocols, such as TCP.

The logical address that IP uses is known as an IP address and looks similar to192.168.3.200—which is different from the physical address (MAC address), which looks like 00-02-3F-6B-25-13. The logical address is responsible for identifying the network the system resides on along with an address of the system, whereas a MAC address is very flat and identifies only the physical system on the LAN—not “where” the system resides.

IP is fully capable of running over either Token Ring or Ethernet networks, as long as an appropriate NIC is used. IP over Ethernet is the most common implementation in networking today, because Ethernet is much less expensive than Token Ring and because TCP/IP is used widely on the Internet.

TCP

The Transmission Control Protocol (TCP) is a transport-layer protocol that is responsible for breaking the data into manageable packets and ensuring that the packets reach their destination. TCP is considered a connection-oriented protocol, which means that it relies on a session being first established. This is different from a connectionless communication, which just sends the data out and if it reaches the destination, great; if not, no big deal. With connection-oriented protocols, a session is established through introductions. Connection-oriented protocols will monitor that session to ensure that the packets have reached their destination.

UDP

The User Datagram Protocol (UDP) is part of the TCP/IP protocol suite. When you send data on a TCP/IP network and if you need a connection-oriented conversation, you have learned you would use the TCP protocol. But what protocol do we use if we want to have a connectionless conversation? UDP. Both TCP and UDP are layer-4 protocols. IP is used to deliver both types of data, but TCP and UDP determine whether it is connection oriented or not.

NFS

The Network File System (NFS) is a protocol for file sharing that enables a user to use network disks as though they were connected to the local machine. NFS was created by Sun Microsystems for use on Solaris, Sun’s version of UNIX. NFS is still used frequently in the UNIX and Linux worlds and is available for use with nearly all operating systems. NFS is a protocol that is used universally by the UNIX community. Vendor and third-party software products enable other operating systems to use NFS. It has gained acceptance with many companies and can be added to nearly any operating system. In addition to file sharing, NFS enables you to share printers. NFS is located in the application layer of the OSI model and is considered a member of the TCP/IP protocol suite. The primary reason to use the NFS protocol is to access resources located on a UNIX server or to share resources with someone working on a UNIX workstation.

SMB and Novell NCP

Microsoft’s Server Message Block (SMB) and Novell’s NetWare Core Protocol (NCP) are protocols that are implemented in redirectors. A *redirector* is software that intercepts requests, formats them according to the protocol in use, and passes the message to a lower-level protocol for delivery. Redirectors also intercept incoming messages, process the instructions, and pass them to the correct upper-level application for additional processing.

SMB and NCP are used primarily for file and printer sharing in Microsoft and Novell networks, respectively, and are considered application-layer protocols.

SMTP

The Simple Mail Transport Protocol (SMTP) is the protocol that defines the structure of Internet mail messages. SMTP uses a well-defined syntax for transferring messages. An SMTP session includes initializing the SMTP connection, sending the destination e-mail address, sending the source e-mail address, sending the subject, and sending the body of the e-mail message.

FTP and TFTP

The File Transfer Protocol (FTP) is a standardized method of transferring files between two machines. FTP is a connection-oriented protocol, which means that the protocol verifies that packets successfully reach their destinations. The Trivial File Transfer Protocol (TFTP) has the same purpose and functions as FTP, except that it is not a connection-oriented protocol and does not verify that packets reach their destinations. By not verifying that data has been successfully transferred to its destination and therefore requiring less overhead to establish and maintain a connection, TFTP is able to operate faster than FTP. TFTP has no authentication mechanism, whereas FTP can require a username and password.

DECnet

DECnet is a proprietary protocol developed by the Digital Equipment Corporation for use primarily in WANs. You can run DECnet on an Ethernet network, but it is done infrequently. DECnet is a routable protocol.

DLC

Data Link Control (DLC) is not a common protocol. DLC, a nonroutable protocol, was sometimes used to connect Windows NT servers to printers.