Overview

Description

This unit contains one lesson:

This lesson will introduce protocols in general. You will look at how a protocol functions, the differences between a routable and a non-routable protocol, what a protocol stack is, and some common protocol stacks. Then you will look specifically at the TCP/IP protocol stack and the most important protocols of TCP/IP: TCP, UDP, and IP. You will also be introduced to IP addressing and the basics of routing.

Unit Table of Contents

This unit contains the following lesson:

<table>
<thead>
<tr>
<th>Lessons</th>
<th>Pages</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lesson 4-1: Introduction to TCP/IP</td>
<td>338-370</td>
<td>5 hours</td>
</tr>
</tbody>
</table>
Lesson 4-1: TCP/IP Protocols

At a Glance

Protocols are the rules and procedures that govern communications between devices on a network. Actually, protocols are found throughout the computer, data communications, and network fields. Protocols are used to define the way in which devices communicate. They govern how a modem and computer communicate, how a video display adapter accesses computer memory, how a file is transferred over the Internet, and how a telephone connects to the telephone network.

With regard to networks, protocols exist for every layer of the OSI model. There are physical layer protocols, data link layer protocols, network layer protocols, and so on. The protocols that operate at each layer offer essentially the same services. However, while the protocols at each layer may provide similar features, how they do their job and what features are implemented varies.

One of the most important sets of protocols in networking today is the TCP/IP protocol suite, often referred to as just TCP/IP. It is the backbone of the Internet and is everywhere—from the smallest to the largest network. TCP/IP is encountered on a Macintosh connected via a modem to the Internet, on a small LAN connected via a router to the Internet, on a corporate intranet, and on a WAN connecting worldwide sites of a large corporation.

There are many protocols that are considered a member of the TCP/IP protocol suite and more have been added or refined over the years. This lesson will discuss only some of the many TCP/IP protocols.

What You Will Learn

After completed this lesson, you will be able to:

- Diagram the relationship of the TCP/IP suite to the OSI model.
- Identify the major protocols of the TCP/IP suite and their features.
- Describe IP addressing and diagram the general structure of an IP address and Classes A, B, and C.
- Explain the practice of subnetting.
**Tech Talk**

- **ARP**—Address Resolution Protocol, is part of the TCP/IP protocol suite and functions between the network and data-link layers of the OSI model to provide IP address to MAC address mappings.

- **ARPANET**—The pioneer long haul (WAN) network funded in the mid-1960’s by the United States Department of Defense’s Advanced Research Projects Agency (ARPA). It is possible to trace today’s Internet directly to the original ARPANET.

- **Best Effort Delivery**—The characteristic of a network that does not guarantee packet delivery. IP is a best effort protocol. Compare with X.25 that guarantees error-free delivery.

- **Domain**—A part of the DNS naming hierarchy. Syntactically, a domain name consists of a sequence of names (labels) separated by periods (dots).

- **Dotted Decimal Notation**—The syntactic representation for a 32-bit integer that consists of four 8-bit numbers (octets) with periods (dots) separating them.

- **Host Address**—The portion of the IP address that designates the host (network device) address rather than the network address.

- **IP Address**—The 32-bit address assigned to hosts participating in a TCP/IP Internet. IP addresses are the abstraction of physical hardware addresses (MAC address) like an internet is an abstraction of physical networks. An IP address is divided into a network portion (Network address) and a host portion (Host address).

- **Multicasting**—The process of sending one message to a group of hosts on a network using the Internet Group Message Protocol.

- **Network Address**—The portion of the IP address that designates the network on which the host resides.

- **Port**—A mechanism, provided by IP, for addressing separate process on a single host machine.

- **Request for Comment (RFC)**—The series of edited, but not referred notes in which the TCP/IP standards are documented.

- **Subnet Address**—A division of the IP addressing scheme allowing a site to divide a single IP network address for multiple physical networks.

- **Subnet Mask**—A bit mask used to select bits from an IP address for subnet addressing. The mask is 32 bits long and selects the network ID.
portion of the IP address and one or more bits of the host portion to identify and divide sub-networks within the IP network.

History of TCP/IP

In the early days of computer networking, networks were an isolated entity referred to as local area networks (LAN). Protocol developers were not concerned with moving data from one network to another. Therefore, early protocols could not move data from one LAN to another. Eventually, these protocols proved inadequate as LANs grew into multi-network configurations called internetworks.

In the late 1960's, the United States Department of Defense Advance Research Projects Agency funded research for a prototype internetwork, the ARPANET. The goal was to build a communications system that could withstand a catastrophic nuclear disaster. Another goal was to encourage communications among major research institutions. The original ARPANET connected four different geographical locations. As it grew, it facilitated communications among major research institutions and the military.

It eventually developed into the Internet, allowing many other computer networks to become connected. These networks were very different from one another, using different equipment and different operating software. This created a need for a “common language” allowing diverse computer networks to communicate and exchange data between LANs. The development of the Internet demonstrated a need for protocols that allowed an internetworking device (e.g router) to determine if data was destined for a local network or for another network on Internet and forward the data accordingly.

In 1974 a UCLA graduate student, Vinton Cerf, and an MIT professor, Robert Kahn, developed the first version of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocols. Over the next 8 years TCP/IP became the standard suite of protocols for inter-computer communications. Although other protocols had strong support at that time, TCP/IP was freely available and was popular at universities. Today, this protocol is the most popular in use.

TCP/IP is actually an entire group of protocols working together to provide multiple, interrelated applications and services. Groups of protocols that work together, such as TCP/IP, NetWare’s IPX/SPX, and AppleTalk, are known as protocol suites. They are also sometimes referred to as protocol stacks.
TCP/IP vs. The OSI Model

The seven-layer OSI model compartmentalizes the process of sending information through a network. TCP/IP at the lower 4 layers follows this model, but combines session, presentation, and application tasks in a single layer. While the tasks performed by TCP/IP are those identified by the OSI model, they are divided somewhat differently.

The reason TCP/IP divides these tasks somewhat differently lies in the development of TCP/IP and the OSI model. TCP/IP was developed in the late 1970’s to address the lack of standards between different systems connected to the ARPANET. The OSI model was developed several years later to address similar issues with increasingly popular local area networks. While the layers and functions of those layers are similar between the OSI model and TCP/IP, there are differences.

- The TCP/IP is a 5-layer protocol stack.
- The TCP/IP application layer combines the functions of the OSI application, presentation and session layers.
- The data link and physical layers are unspecified. TCP/IP supports most LAN technologies (e.g., Ethernet, Token Ring, FDDI).

The figure shows the relationship between the OSI model and TCP/IP.
Check Your Understanding

♦ Why was the TCP/IP suite developed?

♦ What are three differences between the OSI model and the TCP/IP suite?

♦ Diagram the relationship of the OSI models layers to the TCP/IP suite layers.
Overview of TCP/IP Stack

Where the OSI model consists of seven layers, the TCP/IP stack consists of only five layers. The majority of the protocols included in the TCP/IP stack reside in the application layer.

The Application Layer

The TCP/IP application layer is equivalent to the session, presentation, and application layers of the OSI model. In other words, the TCP/IP application layer handles the functions that are specified to occur in these OSI layers. These are the protocols with which you are probably most familiar because they relate directly to the most common processes: email, web browsing, downloading files, and so on.

Other support protocols exist in the application layer to provide host name mapping, booting, and management services.
The Transport Layer

Within the transport layer, the Transmission Control Protocol (the TCP in TCP/IP) provides error free, reliable end-to-end delivery of data. The transport layer also houses the User Datagram Protocol (UDP). UDP is provides less reliable data delivery. It is a connectionless transport service that provides best effort delivery of data. A connectionless service does not provide any guaranteed of delivery.

End-to-end delivery does not stop at the device. Since most systems today are capable of running multiple applications simultaneously, the data must be delivered to the appropriate application. Any application running on a device is called a process. TCP and UDP provide facilities for process-to-process delivery of data.

Transport Layer

[Diagram of OSI and TCP/IP layers]

Application
Presentation
Session
Transport
Network
Data Link
Physical

OSI

Application
Session
Transport
Network
Data Link
Physical

TCP/IP

TCP
UDP
ICMP
IGMP

ARP
IP

Internet
Data Link
Physical
The Internet Layer

At the OSI model’s network layer, TCP/IP provides the Internet Protocol (the IP in TCP/IP). This layer is often referred to within the TCP/IP stack as the internet layer. IP provides the requisite network layer functions to deliver data across networks. This protocol is the backbone of the Internet and provides best effort delivery of data from network to network via a worldwide system of routers. Best effort delivery means that IP does not provide error checking or guaranteed delivery of data.

ICMP reports problems and errors with network devices across the network. IGMP provides the mechanism to send one message to a group of hosts on a network. This process is referred to as multicasting. ICMP and IGMP are encapsulated directly in IP with no TCP or UDP transport association.

Network Layer vs. Internet Layer

![Network Layer vs. Internet Layer Diagram]
Physical and Data Link Layers

Although the typical representation of the TCP/IP stack includes the OSI model’s physical and data link layers, TCP/IP actually operates independently of the physical and data link layer protocols. It supports all standard LAN and WAN technologies (i.e., Ethernet, Token Ring), just as does the OSI model.
TCP/IP Application Protocols

There are many protocols included in the TCP/IP suite which provide services across the Internet. Below are some of the more commonly encountered protocols that reside in the application layer.

HyperText Transfer Protocol (HTTP)

HTTP transfers the HyperText Markup Language (HTML) used to build the web pages accessed on the World Wide Web from the web server to the client's web browser (i.e., Netscape or Internet Explorer) across the Internet. HTML is used to format pages and HyperText links that allows navigation from page to page.

Simple Mail Transfer Protocol (SMTP)

SMTP is the protocol that provides services for sending and receiving email across the Internet. Whenever an email message is sent over the Internet, it is SMTP that handles the transfer of the mail. SMTP specifies that all messages must be text.

File Transfer Protocol (FTP)

FTP is used to copy files between computers over a TCP/IP network. FTP uses the transport services of TCP to provide a reliable, connection-oriented service. It is commonly used when downloading files from the Internet. FTP requires a valid user name and password to access a private FTP server. Anonymous FTP is used to access public FTP servers. With Anonymous FTP, the username is entered as "anonymous" and the password is the user's email address. The computer requesting a file from an FTP server must have an FTP client application installed and the server must have an FTP server application installed. Since FTP relies on the presence of TCP/IP on both the client and the server computers, FTP will work no matter what operating system is on either machine.
Telnet

The Telnet protocol supports remote log-in to a host from another host on the network. Telnet emulates a dumb terminal, much like the old computer terminals connected to mainframe computers. Dumb terminals are computers that have no processing capabilities. They rely on the processing capabilities of the computers to which they are connected. Telnet allows the emulated terminal to make a direct connection to the remote host computer. To make a telnet connection the user must know the domain name or IP address of the remote computer, the login name, and, if required, the password. Once a connection is established, any command typed on the client’s keyboard is sent to the remote computer for execution. Telnet is used in a variety of ways including connecting to a device to configure the device, to control a remote computer, or to manage a remote web server.

Domain Name Service (DNS)

DNS is a centralized directory service that equates a unique name with a host’s IP address. DNS names are used everyday to send emails (jsmith@company.com) or to access a web site (www.anycollege.edu). It is a hierarchy of DNS servers that maintain the lists of host names and IP addresses.

Check Your Understanding

♦ Which application layer protocol provides file copying service?

♦ Which application layer protocol provides terminal emulation?

♦ Which application layer protocol is used to transfer HTML for building web pages?

♦ Briefly describe how FTP and Anonymous FTP are different.
TCP/IP Transport Layer Protocols

Transport layer protocols are responsible for end-to-end delivery of data. The transport layer is also responsible for message segmentation and reassembling the message. User Datagram Protocol (UDP) and its counterpart, Transmission Control Protocol (TCP), both handle these functions within TCP/IP.

User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a connectionless protocol that operates at the transport layer. Two of the primary responsibilities of a transport layer protocol are end-to-end delivery of data and making sure that data is delivered error-free (no loss, duplication, or corruption). UDP handles the first responsibility, but it offers no facilities for ensuring error-free delivery or flow control of the data. Consequently, UDP does not ensure that data will arrive without loss or duplication.

UDP was designed as a fast, low overhead protocol. The packet header in UDP contains fewer bytes than TCP’s header and it has a lower overhead than the more reliable TCP. Consequently, delivery of data is faster. UDP supports higher level protocols that provide error checking and flow control operations or have no need for these services (e.g., DNS).

Upper layer protocols that do not provide these services and yet require these services utilize the more robust TCP protocol.

Transmission Control Protocol (TCP)

Just like UDP, the Transmission Control Protocol (TCP) is responsible for end-to-end delivery of data. TCP is a more complex and robust protocol than UDP. TCP provides a connection-oriented end-to-end delivery.

Unlike UDP, TCP is considered very reliable. It provides error checking, reporting, and complete delivery. As each packet of data arrives, TCP performs a checksum, and reports the success or failure back to the sender. If the packet arrives damaged, the failure is reported and the sender can retransmit the packet.

TCP also perform segmentation of data—the division of a single data message into multiple smaller packets. This sequence control ensures that all packets of the original message are received in the proper order. To do this, TCP includes a sequence number in the header of each packet that is used by the receiver to put the packets in the correct order.

TCP ensures that not only are all packets received error-free and can be put back into their proper order, but that no packets have been lost in transmission. TCP also makes sure that no packets are duplicated.
To ensure that the receiving device is not overwhelmed with a flood of data, TCP provides flow control. If data is coming in too fast, TCP informs the receiver to reduce the data rate until it can catch up.

Compared to UDP, TCP provides reliable delivery, but it also provides slower delivery than UDP due to the added features and packet overhead.

**UDP/TCP Ports**

Since computers are capable of running multiple programs at one time (such as Microsoft Word, Outlook, and a web browser), delivery of data from the source device to the receiving device is not enough. The data must be delivered not only to the receiving device, but to the correct application (or process) as well.

UDP and TCP perform this task by utilizing another level of addressing called a port. Just as a personal computer has a variety of interface ports (i.e., serial and parallel), TCP/IP uses a port to identify different application processes. Each process has a unique port number. For example, when connecting to a Web server, a temporary end-to-end connection is made to port 80, the port number used for accessing Web servers. Port numbers have been defined for many common applications and these port numbers range from 0 to 65535.
Check Your Understanding

♦ Which TCP/IP transport layer protocol is the most reliable? Why?

♦ Briefly describe how TCP and UDP transport data from one process to another.

TCP/IP Internet Layer

The internet layer of TCP/IP directly corresponds to the OSI model’s network layer. This layer provides routing and network addressing functions. The Internet Protocol (IP), the Internet Control Message Protocol, and the Internet Group Message Protocol reside in the internet layer. ICMP reports problems and errors with network devices across the network. IGMP provides the mechanism to send one message to a group of hosts on a network. This process is referred to as multicasting. This lesson will concentrate on the Internet Protocol.

Internet Protocol (IP)

The heart of TCP/IP lies in the Internet Protocol, IP. This protocol provides network layer functionality to move data between networks. IP moves data over any data link and physical layer protocols. This allows an internetwork to be any combination of transmission medium, media access method, physical addressing, or topology.

While a network layer protocol usually guarantees reliable delivery of data, IP makes no such promise. IP is a connectionless protocol. IP provides no error checking and no means by which to report to the sender the outcome of a packet reception. Therefore, IP is also known as a best effort delivery protocol. In addition, data packets that are sent along different routes to reach their destination may arrive out of sequence. While IP does not provide error checking, sequencing, or reporting, its higher-layer partner, TCP, does.

IP Addressing

TCP/IP uses three different types of addressing to move data throughout an internetwork: physical, logical, and port address. TCP/IP utilizes Data Link layer physical addresses to move data within a single LAN. To move data from LAN to LAN across the internetwork, it uses logical addresses. Finally, to move data from end-to-end (process-to-process), a port address is used.
Physical Address (Data Link Layer)

The physical address is the Medium Access Control (MAC) address specified in the Data Link layer frame. Each device on a LAN has a unique MAC address that identifies it on the network. This address is used to move data to the correct device within a single LAN. The MAC address is usually expressed in a 48-bit, Base 16 (Hexadecimal) format (e.g., 00-08-34-F3-87-BC).

Logical Address (Network Layer)

IP provides logical addressing as required by the Network layer to support moving data from network to network independent of the Data Link layer protocol and the physical LAN. Remember that a logical address uniquely identifies a device on an internetwork while a physical address uniquely identifies a device on a particular LAN.

Logical addresses can be represented in Base 2 (binary) format (e.g., 10001110.1101110.11101101.00000001). To make it easier for people to read and understand the logical addresses, they are often written in Base 10 format as four decimal numbers (32 bits), each separated by a dot (e.g., 142.110.237.1). This format is called dotted decimal notation.

The notation divides the 32-bit address into four 8-bit (byte) fields called octets and specifies the value of each field independently as a decimal number.

The IP Address

The network address of the IP address uniquely identifies the network on which the network device resides. Information is routed to a destination network based upon this portion of the IP address. The host address of the IP address uniquely identifies the network device on the destination network. It is used when the packet reaches the destination network specified by the network address.

Addressing Rules

The bits used to define the host portion of an Internet address should not be all one bits. According to the standard, any Internet address with the
host portion consisting of all ones is interpreted as meaning "all", as in "all hosts." For example, the address 128.1.255.255 is interpreted as meaning all hosts on network 128.1.

The bits used to define the network portion of an Internet address should not be all zero bits. According to the standard, a host portion address of all zeros is interpreted as meaning "this," as in "this network." For example, the address 0.0.0.63 is interpreted as meaning host 63 on this network.

**IP Classful Addressing**

There are three primary classes of IP addresses, Class A, Class B, and Class C. Each class allocates a different number of bits to the network and host address.

### IP Class A

Class A addresses allow up to 126 networks and up to 16,777,214 hosts. The first octet of the address is reserved for the network address. The last three octets designate the host address.

**Class A Address Range**

```
Class A: 1.0.0.0 through 126.255.255.254
```

The decimal number in the network portion of a Class A address ranges from 1 to 126. The remainder of the address is the host portion and is assigned by the network administrator.

Class A addresses were assigned to very large corporations and the government during the early days of the Internet. There are no more Class A addresses available for distribution.
Class B addresses allow up to 16,384 networks and 65,534 hosts. The first two octets are reserved for the network address and the last two octets designate the host address.

Class B Address Range

Class B: 128.1.0.0 through 191.254.255.254

The decimal number in the network portion of a Class B address ranges from 128.001 to 191.254. The remainder of the address is the host portion and is assigned by the network administrator.

Class B addresses were assigned to midsize organizations and are also completely allocated.
Class C addresses allow up to 2,097,152 networks and 254 hosts. The first three octets are reserved for the network address and the last octet designates the host address.

**Class C Address Range**

Class C: 192.0.1.0 through 223.255.254.254

The decimal number in the network portion of a Class C address ranges from 192.000.001 to 223.255.254. The remainder of the address is the host portion and is assigned by the network administrator.

Class C addresses are assigned to small organizations. At this writing, there may be some Class C addresses still available, but the availability of Class C addresses is shrinking.

Two additional classes, Class D and E, are reserved for special uses.

**Check Your Understanding**

- Speculate why Class A and Class B addresses are no longer available and why Class C classes are dwindling.
Natural Masks

A host or router uses the leading bits of an IP address to determine its class. When a router tries to forward a packet it looks for the portion of the address that identifies the destination network. A mask tells the router which portion of the address it should look at to find the network. Masks are written in binary. Bits set to one indicate the network portion. Bits set to zero indicate the host portion.

- A Class A address uses the first octet to indicate the network. Its mask is written:
  - 11111111 00000000 00000000 00000000 or 255.0.0.0

- A Class B address uses the first two octets to indicate the network. Its mask is written:
  - 11111111 11111111 00000000 00000000 or 255.255.0.0

- A Class C address uses the first three octets to indicate the network. Its mask is written:
  - 11111111 11111111 11111111 00000000 or 255.255.255.0

Masks for Class A, B, and C addresses are called natural masks.

Subnet Masks and Subnetting

Subnets are logical subdivisions of a single Internet network. For technical or administrative reasons, it is desirable in many organizations to divide the network into several different networks. Routers then connect these independent networks. However, each organization that wishes to connect to the Internet can usually obtain only a single Internet number.

If multiple TCP/IP networks are interconnected across routers, a different network number must be assigned to each network. However, if the network is part of the Internet, any network number cannot be arbitrarily selected. Subnet addressing allows an organization to use a single IP network number for multiple physical networks. Subnets may be used with any Class A, B, or C address.

To identify to the router the different subnets on a network, a subnet mask is created. A subnet mask allows the host portion of an Internet address to be divided into two parts. One part is used to identify the subnet number, and the other part is used to identify a host on that subnet.

A subnet mask looks like a natural mask with more of the bits set to one. The additional ones identify the subnetwork address. As with a natural mask, any bit set to zero is part of the host address. Subnet masks are entered into a router using dotted decimal notation.
For example, a Class B network has the address 134.177.0.0. The first two octets identify the network. If the administrator uses the entire third octet to identify the subnetwork, then the subnet mask is

```
11111111 11111111 11111111 00000000 or 255.255.255.0
```

A Class C network uses the first three octets to identify the network. The last octet can be subdivided so that some of the bits identify a subnet of the Class C and the rest identify the host.

Once the class of an address is determined, the host can easily distinguish between the bits used to identify the network number part of the address, and the bits used to identify the host part of the address.

**Check Your Understanding**

- What is the difference between a MAC address and a logical address in IP addressing?

- Identify how many octets are used for the network address for Class A, B, and C IP addresses.

- Why would an organization want to subnet their network?

- Speculate a solution to the dwindling number of available IP addresses.

**Internet Protocol Version 6**

The IP addressing scheme presented in this lesson is called IP version 4 (IPv4) and it has the shortcoming of running out of addresses in the near future. A new version of IP addressing has been developed that will resolve this problem. IPv6 uses 128 bit addresses instead of 32 bit used by IPv4.
Try It Out

TCP/IP

Materials Needed:

- Sniffer Basic software
- Telnet IP address
- CuteFTP 3.5 Software
- Internet Connection

Telnet

Telnet is a protocol used to perform remote log-in on some distant IP host. TCP uses port number 23 for the Telnet server process. Two IP workstations connected via Telnet form a client server relationship. The device making the request is seen as the client and the one servicing the request is seen as the server. Telnet is used for a variety of reasons; one example might be to connect to an internetworking device such as a router to perform some management function or to execute commands on the remote device.

During this activity you will use the Telnet protocol to connect to a remote PC. Use the ping utility to test network access. Use Sniffer Basic to view each of the protocol’s data structure.

Part 1: Using Telnet

1. Launch Sniffer Basic and start a packet capture session. See Sniffer Basic Help if you forgot how to do this.

2. From the Windows 95 desktop, click the Start button and drag to Run.

3. In the Open dialog box, enter the Telnet (If you do not know the correct IP number, your teacher will provide you with one.) command if you are connected via an Ethernet station.

4. If the Telnet command is successful in connecting to the router, you will see a log-in prompt. TCP must be enabled in order to use Telnet.

5. At the log-in prompt, enter the log-in Id of User (see your instructor) and press Enter.

6. You are now prompted to enter a password; leave the password field blank and press Enter.
7. You should now be at the Technical Interface (TI) prompt of the router. Enter the `dir` command and press Enter.

- What information is displayed?

8. Return to Sniffer Basic and select Capture > End and View.

9. Within the Sniffer Basic capture Summary window, highlight Telnet in the layer column of that window.

10. View the capture information for that packet. You should see multiple layers of protocol headers that relate to the OSI seven-layer model.

- What protocols are present?
- What layers of the OSI seven-layer model do they represent?

**Viewing the Routing Table**

1. Minimize Sniffer Basic and return to the Telnet window.

2. You should now be at the Technician Interface (TI) prompt. Enter the `show ip route` (case sensitive) command and press Enter to display the routing table.

- How many entries are there in the Routing Table?

**Viewing the Router’s ARP Cache**

At the Technician Interface prompt, enter the `show ip arp` command and press Enter to display the ARP Cache.

- How many entries are there in the ARP Cache?
- Is your IP address and MAC address present?

**Rubric: Suggested Evaluation Criteria and Weightings**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Problems, successes, and/or comments entered in Portfolio</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Accurately follows directions</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Completeness and accuracy of answers to lab questions</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100</strong></td>
<td></td>
</tr>
</tbody>
</table>
Part 2: Using FTP

File Transfer Protocol (FTP) is a protocol used to transfer files between IP nodes. It uses the transport services of TCP so that it provides a reliable (connection-oriented) service. It is very commonly used when downloading files from the Internet. It is well suited for transferring large files, due to its reliable services, and is therefore well suited for use over WAN links.

FTP uses two well-known TCP port numbers, 20 and 21. Port 21 is used for the control information and the actual data is transferred via port 20. In addition, it has provisions for log-in authentication, such as user name and password. Anonymous FTP allows the user to log in to public FTP servers as “anonymous” and to use their email address as the password.

1. Launch Sniffer Basic and start a packet capture session.
2. From the Windows 95 Desktop, click the Start button and drag to Programs.
3. From the Programs menu, click GlobalSCAPE, and then click the CuteFTP program icon.
4. After CuteFTP has opened, click the FTP menu command and drag down to Quick Connection.
5. When the connection screen opens, enter the following information at each prompt:
   a. At the Host Address box, enter internic.net.
   b. At the Log-in box, enter anonymous.
   c. At the Transfer type box, enter Auto-Detect.
6. Click OK.
7. In FTP, a file folder is actually called a directory. Once connected, drag the scroll bar down to the rfc directory, and double click. This will open the rfc directory.
8. Locate within the rfc directory the file named rfc1122.txt. This file is the Request for Comments (RFC) documenting the TCP/IP Protocol Suite.
9. Double click on the rfc1122.txt file. Downloading will occur immediately into the CuteFTP folder located on your PC’s hard drive.
10. Once the downloading is finished, click on the FTP menu and select Exit.

12. Double click to open the document. It will open as a Wordpad document.

13. Study the document on the screen. The document is too large for everyone in your class to print.

14. This lesson represents an overview only of the TCP/IP protocol suite. From your study of the actual TCP/IP RFC, write a short paper (1-2 pages) on the additional information gained from reading and studying the RFC.

Rubric: Suggested Evaluation Criteria and Weightings

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Successful download of the TCP/IP RFC</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Thorough analysis and synthesis of new knowledge of TCP/IP</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>100</strong></td>
<td></td>
</tr>
</tbody>
</table>
Stretch Yourself

HTTP Revealed

Materials Needed

- Internet connection
- Netscape Communicator Web Browser or similar

Start by using your WWW browser to verify that you can reach several web sites. Try connecting to http://www.nortelnetworks.com/. Start the Telnet application.

Use the "Remote System" entry from the "Connect" menu to open the Connect dialog. In the area asking for the name of a host, type: www.nortelnetworks.com. In the area asking for a Port (it probably contains the word "Telnet" now), type "80". In the TermType area make sure VT100 is displayed. Now push the connect button.

Wait a few moments. You will not see any confirmation of a connection, but if you don't get an error message saying the connection failed, you are connected.

Put your cursor in the Telnet window, and carefully type:

GET /index.html HTTP/1.0

Next, press the enter key twice. You must type very carefully, because you will not be able to see what you are typing. Don't worry, eventually you will! You must type the command above exactly as it appears. Case is important. So are the two enters.

Can you make any sense of what you see? Compare it to what you see in the Netscape Communicator browser. In the Netscape Communicator browser, under the View menu you can choose "Page Source" to view the HTML used to create Nortel Network's web page. Compare it to what you saw in the Telnet window.
What do you think is happening? Experiment with other two other sites of your choosing. Document your results.

Write a short summary of your experience, results, and speculations.

**Rubric: Suggested Evaluation Criteria and Weightings**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Documentation of results from three sites.</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Short summary with thoughtful speculations about the results.</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>
Network Wizards

SMPT

Materials Needed

- Internet connection
- Name of the machine that your school uses as its email relay

Sending Mail with SMTP

In this activity, you will explore SMTP, the Simple Mail Transfer Protocol. To do this, you will have to find out, from your system administrator or instructor, the name of the machine that your site uses as a mail relay.

Port 25 is the well-known port for SMTP, Internet email. Try connecting to your mail relay, as you did in the Try It Out section. This time, instead of port 80, use port 25.

Again, you will not be able to see what you type, so you must type very carefully. Once you are connected, type:

HELO name

and press Enter. Instead of typing "name," type your first name. You should get a reply from the mail server. Look carefully at it. Can you figure out what any of it means?

Next, type:

MAIL FROM: your-email-address

and press Enter. Use your own email address. The mail server should reply with something like:

250 Sender Ok

Next, type:

RCPT TO: your-email-address

and press Enter. Again, use your own email address. This time the mail server should reply with:

250 Recipient Ok

Next, type:

DATA
The server should say:

354 Enter mail, end with a "." on a line by itself.

Type a short message, and end it by typing "return", ".", "return".

The server should reply:

250 Message accepted for delivery.

Check your mail to and see if have received the new message.

Did you notice that each of the responses from the server began with a number? What do you suppose those numbers are? Why do you think they are there?

Write a short summary of your experience, results, and speculations or answers to the questions above.

Rubric: Suggested Evaluation Criteria and Weightings

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Successful email delivery</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Short summary with thoughtful speculations or answers to questions.</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

Summary

In this lesson you learned the following:

- The relationship of the TCP/IP suite to the OSI model.
- The major protocols of the TCP/IP suite and their features.
- IP addressing and the general structure of an IP address and Classes A, B, and C.
- The practice of subnetting.
Review Questions

Lesson 4-1: TCP/IP Protocols

Part A
1. Create a diagram that illustrates the relationship of the TCP/IP protocol suite to the OSI model.

Part B
1. List the major protocols that reside in the application layer of TCP/IP.
2. List the major protocols that reside in the transport layer of TCP/IP.
3. List the major protocols that reside in the internet layer of TCP/IP.
Match the protocol to its corresponding services.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>IP</td>
<td>A. A connectionless protocol that provides fast data delivery for applications that do not need error checking.</td>
</tr>
<tr>
<td>2.</td>
<td>TCP</td>
<td>B. Used to copy files across a TCP/IP network regardless of the hosts' operating system.</td>
</tr>
<tr>
<td>3.</td>
<td>DNS</td>
<td>C. Sends error messages and reports to the Internet Protocol.</td>
</tr>
<tr>
<td>4.</td>
<td>Telnet</td>
<td>D. Transfers the HTML that is used to build web pages.</td>
</tr>
<tr>
<td>5.</td>
<td>ICMP</td>
<td>E. Centralized directory service that equates a unique name with a host’s IP address.</td>
</tr>
<tr>
<td>6.</td>
<td>UDP</td>
<td>F. A best effort protocol that provides routing and network addressing functions.</td>
</tr>
<tr>
<td>7.</td>
<td>HTTP</td>
<td>G. Provides services for sending and receiving emails across the Internet.</td>
</tr>
<tr>
<td>8.</td>
<td>FTP</td>
<td>H. Provides the mechanism to send one message to a group of hosts on a network.</td>
</tr>
<tr>
<td>9.</td>
<td>IGMP</td>
<td>I. A connection-oriented protocol that provides error checking, flow control, sequencing, and controls for lost or duplicated packets as part of its data delivery system.</td>
</tr>
<tr>
<td>10.</td>
<td>SMTP</td>
<td>J. Supports remote login to a host from another host on a network.</td>
</tr>
</tbody>
</table>
Part C

1. What are the two components of an IP address?

2. Diagram the general configuration of an IP address.

3. What is the purpose of a MAC address?

4. Explain how the logical address of a network device is represented.

5. Create general diagrams that represent Class A, B, and C IP addresses.
   Class A:

   Class B:

   Class C:
6. What is the network address range of a Class A address?

7. What is the network address range of a Class B address?

8. What is the network address range of a Class C address?

9. What are the natural masks for Class A, B, and C?

10. What solution has been developed to increase the number of IP addresses available? How does this solution work?

**Part D**

1. Explain why subnetting is necessary.

2. Briefly describe how a subnet is created.
### Scoring

**Rubric: Suggested Evaluation Criteria and Weightings**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>%</th>
<th>Your Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part A: Diagram the relationship of the TCP/IP suite to the OSI model.</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Part B: Identify the major protocols of the TCP/IP suite and their features.</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Part C: Describe IP addressing and diagram the general structure of an IP address and Classes A, B, and C.</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>Part D: Explain the practice of subnetting.</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>100</td>
<td></td>
</tr>
<tr>
<td><strong>Try It Out:</strong> TCP/IP</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td><strong>Stretch Yourself:</strong> HTTP Revealed</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td><strong>Network Wizards:</strong> Send mail with SMTP</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td><strong>FINAL TOTAL</strong></td>
<td>400</td>
<td></td>
</tr>
</tbody>
</table>

### Resources
