

Module 7

Transmission Control Protocol Internet Protocol (TCP/IP)

7.1 OBJECTIVES

Students will be able to:

- Define the role of Transmission Control Protocol/Internet Protocol (TCP/IP)
- Outline the role of TCP/IP components; TCP, IP, UDP
- Distinguish between the three classes of TCP/IP addresses
- Explain function of Dynamic Host Configuration Protocol (DHCP)
- Describe Windows Internet Name Service (WINS)
- Describe Domain Name Server (DNS)

7.2 OVERVIEW

TCP/IP is the default network protocol for the Intel installation of Windows NT 4.0. TCP/IP is also the only protocol that is supported on the Internet, making it global in scope. NT is equipped with three services to assist in implementing TCP/IP: Dynamic Host Configuration Protocol (DHCP), Domain Name Server (DNS), and Windows Internet Name Service (WINS).

This module will provide a detailed explanation of TCP/IP, as well as how it is configured and implemented. We will also look at the fundamentals of DHCP, DNS, and WINS.

7.3 TCP/IP HISTORY

The Internet was originally proposed by the Advanced Research Projects Agency (ARPA) as a way to connect national computers across the country. The net was called ARPANET, with four switching nodes located at various sites nationwide. TCP/IP was created in the late 1960s as a way to transmit network packets that contained information across the network. As ARPANET grew out of a military-only network to add subnetworks in universities, corporations, and user communities, it became known as the Internet. However, there is no single network called the Internet. The term refers to the collective network of subnetworks. The one thing they all have in common is TCP/IP as a communications protocol.

TCP/IP became important when the Department of Defense (DoD) and universities across the country began to use it as the de facto standard on the Internet. TCP became the industry standard because it is an open protocol capable of working on a variety of different platforms. Although it is the industry standard, it is the hardest protocol to configure.

7.4 TCP/IP

TCP/IP is a software-based communications protocol suite used to transmit data packets across networks. Although the term TCP/IP implies a combination of two protocols, it is actually a large set of software programs, including services and utilities, that provide network services, such as remote login, remote file transfer, and electronic mail.

TCP/IP is the portion of the software part of the suite that provides connection-oriented communications between networks. Connection-oriented and connectionless traffic both refers to the reliability of the received data across a network. Connectionless traffic does not guarantee that the data transmitted will

ever reach its destination, nor does it guarantee the reliability of the data once it is received. Connection-oriented traffic refers to a higher level protocol that uses a connectionless protocol for transmission. IP is the portion of the TCP/IP suite that provides for the connectionless transmission of data packets. TCP/IP is responsible for assembling data passed from higher-layer applications into standard packets and ensuring that the data is transferred correctly. TCP implements the mechanisms required for error checking and reordering missing packets, providing reliable transmission of data packets from one network to another.

Despite being a difficult protocol to configure, TCP/IP has many advantages:

- TCP/IP is a routable protocol; therefore, useable on Wide Area Networks (WANs)
- TCP/IP is the language of the Internet
- TCP/IP is a widely accepted open standard
- TCP/IP is portable

7.4.1 TCP/IP COMPONENTS

There are many protocols that make up the TCP/IP protocol suite. Each protocol in the suite is responsible for performing a specific task.

- **Transmission Control Protocol (TCP):** TCP is an internetwork connection-oriented protocol that corresponds to the OSI Transport layer. TCP provides full-duplex, end-to-end connections.
- **Internet Protocol (IP):** IP is a connectionless protocol that provides datagram service, and IP packets are most commonly referred to as IP datagrams. IP is a packet-switching protocol that performs the addressing and route selection.
- **File Transfer Protocol (FTP):** Windows NT 4.0 provides a graphical Telnet utility that allows connectivity to any other system using a standard Telnet server. The connection can be anywhere on the local network or on another network anywhere in the world, as long as the user has permission to log onto the remote system.
- **User Datagram Protocol (UDP):** UDP is a connectionless Transport (host-to-host) layer protocol. UDP does not provide message acknowledgement; rather, it simply transports datagrams.
- **Windows Internet Naming Services (WINS):** WINS provides a function similar to that of DNS, with the exception that it provides NetBIOS names to IP address resolution.
- **Simple Mail Transfer Protocol:** SMTP is used for transferring electronic mail and is completely transparent to the user. SMTP connects to remote machines and transfers mail messages much like FTP transfers files.
- **Domain Name Service:** DNS enables a computer with a common name to be converted to a special network address. For example, a PC called Langley cannot be accessed by another machine on the same network unless some method of checking the local machine name and replacing the name with the machine's hardware address is available. DNS provides a conversion from the common local name to the unique physical address of the device's network connection.

- **HyperText Transfer Protocol (HTTP):** HTTP is one of the most widely used protocols for transferring information on the Internet. HTTP is used to transfer information from web servers to web browsers.

7.5 TCP/IP ADDRESSING

Any type of network that communicates between computers must have a unique way of distinguishing between computers. At the lowest level, the serial numbers actually burned into the network adapter card are used to identify different computers (This is called the MAC address).

There are two main forms of addresses: a node address and logical network address. A node address is the address of the entity or device on the network, whereas the logical network address is the segment on the network to which the node is attached.

To make TCP/IP work, each and every device on a TCP/IP network requires a unique address. An IP address identifies the device to all the other devices on the network. IP addresses are made up of two parts. The first identifies your network ID. With the Internet spanning the entire globe, every network or part of a network must have a unique ID.

This ID is used to route the information being sent to the correct network. The other part of your IP address is the host ID, a unique number that identifies each computer and device on your network that talks using TCP/IP. Think of the Network ID as your organization, for example, the 555th Comm Squadron and the Host ID as your individual PC. See table 7-1 for a breakdown of this for the different classes.

TCP/IP uses a unique numbering scheme that encapsulates the network and node address into a set of numbers. This number is what is known as an IP address. An IP address is a set of four numbers, or octets, which can range value between 0 and 255. Each octet is separated by a period. Some examples of TCP/IP addresses are:

- 34.120.66.79
- 20.200.20.2
- 2.5.67.123
- 107.219.2.34

TCP/IP addresses are actually broken down into three distinct classes. These are known as Class A, B, and C addresses.

- **Class A** IP addresses contain a number between 1 and 127 before the first dot. Some examples are 3.3.6.8, 102.100.77.8, etc. In a class A address, the first octet represents the network address, and the last three octets represent the node or host number. A class A address can have up to 17 million different hosts.

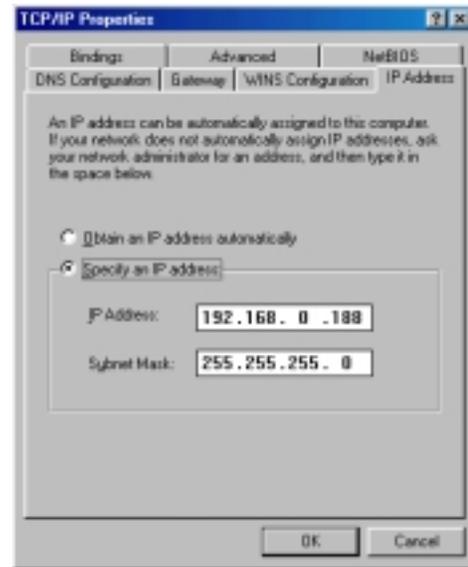


Figure 7-1. Example of IP Address and Subnet Mask

- **Class B** IP addresses follows a similar principal to a Class A address. The first octet can range in value from 128 to 191, but it is the first two octets that make up the network address, and the last two octets make up the host ID. This class can have up to 65,000 different hosts per network.
- **Class C** IP addresses uses the first three octets for the network ID and the last octet represent a host. A Class C address has a first octet value from 192 to 223. This allows 256 different hosts per address.

| Class | IP Address | Network ID | Host ID |
|---------|--------------|--------------|-----------|
| Class A | 102.44.7.100 | 102.0.0.0. | x.44.7.10 |
| Class B | 131.107.4.6 | 131.107.0.0. | x.x.4.6 |
| Class C | 200.9.88.250 | 200.9.88.0 | x.x.x.250 |

Table 7-1. Classes and Addresses

7.5.1 Subnet Mask

In order to determine where to divide the IP address into left and right, a subnet mask is used. A subnet mask is also a 32-bit value expressed as four octets. By reading the subnet mask, the system can determine which portion of the IP address is the Network ID, and which is the Host ID.

- **Class A:** The subnet mask for Class A would be: 255.0.0.0
- **Class B:** The subnet mask for Class B would be: 255.255.0.0
- **Class C:** The subnet mask for Class C would be: 255.255.255.0

7.6 CONFIGURATION RULES

Addressing requirements for IP configuration is quite complex. However, there are four cardinal rules every manager needs to know:

1. Host IDs cannot be set to all zeros or all ones. All zeros or ones in a Host ID denote a broadcast message.
2. Host IDs cannot use 127 in the first octet of an address. 127 are recognized as a special diagnostic address, called a loop back address. Any address using 127 in the Host ID is automatically returned to the sending address as a way to test the network configuration.
3. All Net IDs must match. If a NIC does not have the same Net ID as the rest of the NICs on its subnet, it will not be able to communicate with them. If it does not have the same Host ID as the other NICs on the subnet, it will not be routed to the proper subnet.
4. All Host IDs on a subnet must be unique. If an NT computer attempts to join the network with a duplicate Host ID, it sends a message indicating a duplicate IP address is being used. The duplicate computer is not allowed to join the network. If a non-Windows host joins the network with a duplicate Host ID, serious problems will occur, including intercepting the wrong data packets.

7.7 IPV6

Since the popularity of the Internet has grown, we are running out of TCP/IP addresses. The current version of IP (IPV4) provides for 4 billion 32-bit addresses. It is estimated that these addresses will run out by about 2010. IPV6 is 128 bits long, or four times than an IPv4 address. That doesn't mean there are only four times as many addresses; it means there are an ENORMOUSLY number of IPv6 addresses, because we're talking about exponential growth.

7.8 DHCP

Dynamic Host Configuration Protocol (DHCP) is an open-standard protocol that allows the assigning of IP addresses dynamically via a server. The need for DHCP and its capabilities are numerous. Many times, administrators become so busy that they do not accurately document IP address, resulting in duplication of addresses being assigned. Duplicate addresses can cause problems from the malfunctioning of a single workstation to the downing of an entire network. A computer being moved from one subnet to another causes another common problem. If a computer moves from one subnet to another without updating the IP address, it will not be able to connect to the network. Benefits of using DHCP include:

- Centralized administration. All of your IP addresses, along with your configuration parameters, are stored in a central database located on the DHCP server
- Automatic TCP/IP address assignments and configuration
- Automatic return of unused TCP/IP addresses to the available pool of addresses

DHCP is like a recyclable paper plate. This protocol is a client/server solution for sharing numeric IP addresses. The DHCP paper plate (DHCP server) maintains a pool of shared addresses and those addresses are recyclable. When a DHCP client computer wants to use a TCP/IP application, the client must first request an IP address from the DHCP server. The server checks the shared supply; if all the addresses are in use, the server notifies the client that it must wait until another client finishes its work and releases an IP address. If an address is available, the DHCP server sends a response to the client that contains the address.

This is a good general idea of how DHCP works, but in more detail this is how it works.

1. **You turn on your computer.**

TCP/IP starts, but remember, you're a traveler. You have no permanent IP address.

2. **Your DHCP client software asks to lease an IP address.**

This request is called a DHCP discover message. The DHCP discover message contains the name of your computer and its hardware address. Your hardware address come on your Network Interface Card (NIC).

3. **Your computer keeps broadcastings its lease request until a DHCP server responds.**

If there's no DHCP server – maybe an earthquake destroyed it – your computer keeps trying, but never gets its address. That means you can't use any TCP/IP applications or services.

4. **All the available DHCP servers answer your message by offering your proposed IP address, the servers' IP address, a subnet mask, and the duration of the lease in hours.**

Your computer grabs an IP address so that no one else can take it while you're negotiating.

5. **Your DHCP client takes the first offer and broadcasts its acceptance.**

The other servers cancel their offers.

6. **Your selected DHCP server makes an IP address permanent and sends you an "acknowledged" message (DHCPACK).**

7. **You have an IP address.**

You can use TCP/IP applications and services as long as you want – or until your lease expires.

Usually a DHCP server renews your lease with no problem. In fact, you don't have to do anything. The entire process is automatic and doesn't interfere with what you're doing.

This shared-supply approach makes sense in environments in which computers don't use TCP/IP applications all the time or in which there aren't enough addresses available for all computers that want them.

7.9 WINS FUNDAMENTALS

Microsoft provides WINS as an alternative to DNS for resolving names to IP addresses. WINS replace the need for local host files, DNS databases, and DNS servers. WINS is designed to be easier to set up and manage than DNS databases.

WINS is fine for Microsoft-based networks that aren't connected to the Internet. WINS can work together with DNS, but if you're going to DNS anyway, for example, to run a name server that's connected to the Internet, why use both? You would need to maintain databases for both and monitor both for performance.

Windows Internet Name Service is the resolution service used in a TCP/IP network. The primary function of WINS is to Resolve and Register. It resolves NetBIOS computer names to IP addresses, and then registers them in a dynamic database.

Anytime you use Explorer or Network Neighborhood you are using the NetBIOS interface. It is important not to confuse NetBIOS names with Host names. A Host name is a convenient substitute for numeric addresses. A NetBIOS name is a mandatory unique name used for most Microsoft network functions. Where DHCP is a true cross-platform service, WINS is strictly a Windows- and DOS-only artifact. The NetBIOS name space is flat, not hierarchical; therefore, there is no way to distinguish between a server called Instructor on the Class_1 domain and a server called Instructor on the Class_2 domain. For this reason, every computer must have a unique name on the network. A WINS server resolves these problems and registers the names to an address in a database.

The benefits of using a WINS server include:

- **Centralized management:** Using the WINS Manager, you can administer other WINS servers and designate replication partners. A replication partner is used to replicate the database

between servers so that every WINS server has a complete listing of every client's name and address.

- **Dynamic address mapping and name resolution:** Every time a WINS client starts, and at specified intervals thereafter, the WINS client registers its name with the WINS server.
- **Domain wide browsing:** If you are using a WINS server, your clients can browse for computer resources on a Microsoft network across a router without needing an NT domain controller.
- **Reduction of broadcast traffic:** A WINS server decreases the number of broadcast messages by supplying an IP address when a name query message is received for a computer name from its local database on a WINS server.

7.10 DNS

The Domain Name Service is used to resolve host names to IP addresses. Unlike NetBIOS names, which are required for all NT computers, host names are optional and are used to avoid having to remember long IP addresses. It is much easier to remember `www.whitehouse.gov` than `198.137.240.91`.

DNS is a client/server environment. The clients issue queries, asking a name server for a computer name-to-numeric address translation. If the name server can answer the query, it responds with the requested information.

If the name server can't supply the information, two things may occur, based on whether the name server is or is not responsible for the information.

- If the name server is responsible for the information, it responds with a message that indicates the information doesn't exist.
- If the name server isn't responsible for the information, it forwards the query to, or at least toward, the name server that's responsible. The name server knows to do this based on how the system manager has set things up. When the answer comes back, it travels all the ways back down the chain to the client. This is called a recursive search.
- If the client "times out" – gets tired of waiting for a response that's the same as receiving a "No information" answer from the queried name server.

7.10.1 PIECES AND PARTS OF DNS

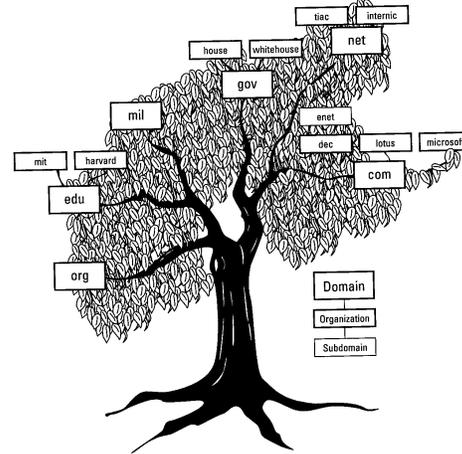
Lots of bits and pieces that work together for DNS, including hardware, software (programs and some TCP/IP protocols), data files, and people.

- The **distributed database** holds information about computers in domains on the Internet or on your Internet.
- **Domains** are logical collections of computers whose requests for network address lookups are all handled by the same server(s).

- **Name servers** are programs that request network address information from the name servers.
- The **resolver** works on behalf of the client applications to get network address information from the name server.
- **System managers and network administrators** set everything up and maintain the databases.

7.10.2 DOMAINS

The Internet is so huge that it organizes its participating computers into groups of administrative units called domains. The domains themselves are organized hierarchically into a tree structure as illustrated in Figure 7-2



The Internet’s tree structure has branches extending from the top-level domains. Your computer sits in the leaves, at the edge of this hierarchy of domains. The InterNIC establishes and maintains the domain at the root of this tree. Just above the root is the set of top-level domains.

The InterNIC is an organization that establishes and maintains the domain at the root of this tree.

Figure 7-2. Hierarchical Structure of Internet domains

7.10.2.1 DOMAIN REGISTRATION

The InterNIC (www.rs.internic.net) charges \$70.00 to register a domain name in some of the top-level domains shown in Table 7-2. The annual maintenance fee is \$35.00. To register a site in the .gov domain go to www.registration.fed.gov and to register a US military agency, go to the registry at www.nic.mil.

| Organization Type | Definition |
|-------------------|---------------------------|
| com | Commercial enterprise |
| edu | Educational enterprise |
| gov | United States Government |
| org | Organization |
| mil | Military Service |
| net | Network services provider |

Table 7-2. Top-Level Domain Names in the United States

Outside the US, the rightmost piece of the Internet address is the two-character country code specified by ISO standard 3166; a few of these top-level domains are listed in Table 7-3.

| Country code | Country |
|--------------|---------|
| ca | Canada |
| in | India |

| | |
|----|--|
| uk | United Kingdom (Actually, the ISO code is gb, but it's hard to make a long story short about whether a country is in Great Britain or the UK.) |
| us | United States |

Table 7-3. Some International Top Level Domains

7.10.2.2 SUBDOMAINS

The top-level domains branch out into subdomains, which are usually named after your organization. A subdomain is any subdivision of a domain. So a subdomain of a top-level domain is a second-level domain. If your organization is large, it may further create its own subdomains for administration purposes.

7.10.2.3 FULLY QUALIFIED DOMAIN NAMES

Each DNS domain has a unique name. This name is so important that it actually becomes part of each computer's name. The result is called a fully qualified domain name, or FQDN.

Here are some examples:

- The computer named **hbs** is part of the DNS domain named **harvard.edu**, yielding the FQDN **hbs.harvard.edu**
- The mythical computer name **viper** is part of the mythical DNS domain name **support.lotus.com**, yielding the FQDN **viper.support.lotus.com**

7.11 VIRTUAL PRIVATE NETWORK (VPN)

Network security is increasing in importance for companies of all sizes. Whether to protect information in transit in remote access sessions, branch network connections, or internal networks, solutions for this form of security are essential.

In general, security is not a single product or technology but an integration of several technologies combined with management policy that provides protection balanced with acceptable risks.

Microsoft Windows operating systems include technology to secure communications over private and public networks. This technology is called a Virtual Private Network (VPN). Currently, Microsoft provides tools to provide security services at the link and transport layers, as well as providing application-layer security for electronic mail. Link layer security encrypts data in transit within remote access sessions as well as within branch network connections. Transport layer security permits protection of TCP-based protocols, including World Wide Web sessions. The Windows Network operating system will provide end-to-end network layer security services through Internet Protocol (IP) Security (IPSec), which permits security services to be applied on internal networks.

7.11.1 PROTOCOLS FOR SECURE NETWORK COMMUNICATIONS

Over the past few years, a number of protocols have emerged that are categorized as VPN protocols and that encrypt communications. These include:

- *Internet Protocol Security (IPSec)*—an architecture, protocol, and related Internet Key Exchange (IKE) protocol, which are described by IETF RFCs 2401-2409.
- *Layer 2 Forwarding (L2F)*—created by Cisco Systems.
- *Layer 2 Tunneling Protocol (L2TP)*—a combination of PPTP and L2F, which evolved through the IETF standards process.
- *Point-to-Point Tunneling Protocol (PPTP)*—Created by the PPTP Industry Forum (US Robotics (now 3Com), 3Com/Primary Access, Ascend, Microsoft, and ECI Telematics).

While IPSec, L2TP, and PPTP are viewed by many as competing technologies, each offer different capabilities that are appropriate for different uses. Breaking down each VPN protocol goes beyond the scope of this training, but it is important to understand that they exist and can be used in combination to achieve secure communications.

7.12 TOPOLOGIES

Topologies can be broken down into two methodologies, physical and logical. A physical topology describes the tangible layout of media (wires) and nodes that are networked together. A logical topology simply describes how information or data flows within a network.

Microsoft NT supports the following Physical topologies:

- Bus
- Star
- Ring
- Mesh

The Star, Figure 7-3, and Bus, Figure 7-4, are the two most common physical topologies in use today.

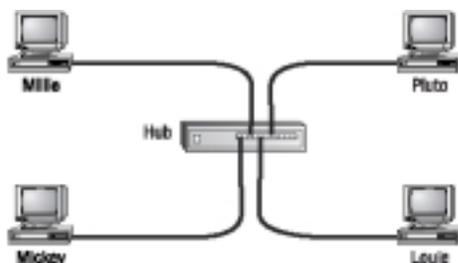


Figure 7-3. Physical Star Topology

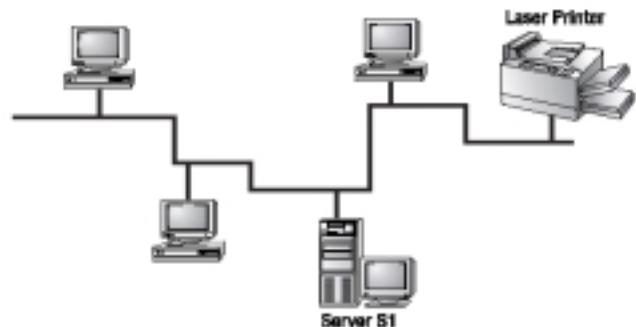


Figure 7-4. Physical Bus Topology

The ring physical topology, Figure 7-5, is more apt to be utilized as the backbone for large networks.

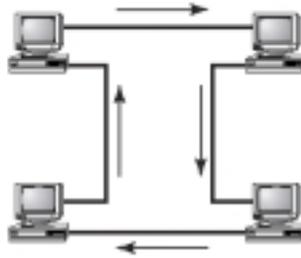


Figure 7-5. Physical Star Topology

7.13 SUMMARY

Although TCP/IP is a versatile and universal protocol, it does require considerable administration to make sure it performs correctly. This module covered the basic components of TCP/IP and the Windows NT tools used to manage them. One significant tool is DHCP, which reduces error and administrator workload by automatically assigning IP addresses to DHCP clients. Since computers may sometimes change their IP addresses, NT includes WINS, which can dynamically register the proper IP address to the computer's NetBIOS name. WINS also significantly reduce network broadcast traffic due to NetBIOS name registration and resolution queries. DNS is used to resolve the difficult to remember IP addresses with computer host names. When used in conjunction with WINS, it can also provide dynamic name and address resolution.

