Microsoft®

Module 1: Reviewing the Suite of TCP/IP Protocols

Contents

Instructor Notes

Presentation:
70 minutes

Lab:
00 minutes

This module provides students with a review of the ISO Open Systems Interconnection (OSI) reference model and the suite of Transmission Control Protocol/Internet Protocol (TCP/IP) protocols. Understanding the function of each protocol in the TCP/IP protocol suite and how the protocols relate to each other and to the OSI model provides students with the fundamental knowledge to perform common network administration tasks.

After completing this module, students will be able to:

- Describe the architecture of the OSI reference model and the function of each layer.
- Describe the four layers of the TCP/IP protocol suite.
- Capture and view frames by using Network Monitor.

Required materials

To teach this module, you need the Microsoft® Office PowerPoint® file 2276C_01.ppt.

Important It is recommended that you use PowerPoint 2002 or later to display the slides for this course. If you use PowerPoint Viewer or an earlier version of PowerPoint, some features of the slides might not be displayed correctly.

Preparation tasks

To prepare for this module:

- Read all the materials for this module.
- Complete the practices.
- Read the referenced requests for comment (RFCs).

How to Teach This Module

This section contains information that will help you to teach this module.

Lesson: Overview of the OSI Model

This section describes the instructional methods for teaching this lesson.

What Is the OSI Model?

Emphasize to students that, although they do not actually use the OSI model to complete a task, understanding the concepts that the model describes is essential to their understanding of network communication systems.

Multimedia: The Layers of the OSI Model

Review the analogy that is used in this presentation to help students understand the OSI model.

This presentation suggests that the creating, packaging, and transmitting of data over a network is analogous to writing a document and sending it by a delivery service. This analogy might not be entirely suitable in some places, such as the translation of the document into the recipient's language at the presentation layer.

OSI Network Communication

Explain what each layer of the OSI model does as the request is passed from the client computer to the database server. Provide additional examples of data movement, such as file transfers, to show that the function of each layer is consistent.

The OSI Model and Network Devices

Explain to students why each type of device operates at the OSI layers listed. In particular, ensure that students understand the difference between traditional layer 2 switches and advanced switches that operate at layer 3 or layer 4. This is terminology used by vendors and shows the relevance of the OSI model.

Lesson: Overview of the TCP/IP Protocol Suite

This section describes the instructional methods for teaching this lesson.

Multimedia: Why Do I Need to Know About TCP/IP?

This presentation uses live action and animation to describe the kinds of tasks that students, as administrators, might be required to perform—tasks that require an understanding of TCP/IP. Use the presentation as the introduction to a short discussion with students about opportunities they have had to work with TCP/IP or where they anticipate needing a better understanding of TCP/IP.

Discuss the five screens described in the presentation and emphasize to students that, at the completion of this course, they will have all the information they need to understand the configurations depicted in these screens.

What Is the Architecture of the TCP/IP Protocol Suite?

Emphasize to students that, just as with the OSI model, understanding the architecture of the TCP/IP model and the functions of the protocols in the TCP/IP protocol suite is crucial to their understanding of network communications systems. Advise students that RFC 1180 includes a tutorial that describes the TCP/IP protocol suite.

What Is an RFC?

Emphasize that the RFC process is an open process in which anyone can participate. Be sure that students understand that, although an RFC can be useful for reference, vendor documentation is used to find implementation details of specific products.

How Does the TCP/IP Model Relate to the OSI Model?

Focus on reviewing where the protocols operate in the four-layer TCP/IP model and how the TCP/IP model relates to the OSI model. The multimedia piece that follows this topic describes the protocols in more detail.

Multimedia: Network Communication Using the TCP/IP Protocol Suite

This presentation is divided into sections. Briefly review each section before continuing with the next. Repeat a section if students need to see it again.

TCP/IP Network Communication

Explain what each protocol in the TCP/IP protocol suite does during the communication process between a Web client and Web server. Stress to students that, unlike the OSI model, each protocol here is actually implemented as software.

Practice: Overview of the TCP/IP Suite

In this practice, student associate protocols with different layers of the OSI model. This practice is multimedia-based. Be sure that students understand how to start the practice from their Student Materials compact disc.

Lesson: Viewing Frames by Using Network Monitor

This section describes the instructional methods for teaching this lesson.

What Is Ping?

The Ping utility (Ping) is introduced here so that students can generate a sample of network traffic for analysis. Most students are likely to be familiar with Ping, so do not spend much time on this topic.

What Is ARP?

Address Resolution Protocol (ARP) is introduced here so that students can understand ARP packets when viewing them in Network Monitor. The ARP utility is introduced so that students can understand why they are clearing the ARP cache in the practice.

How ARP Resolves IP Addresses to MAC Addresses

Explain each step of the ARP process as the step is completed on the slide. If students are comfortable with this material, consider enhancing the presentation by explaining why ARP will find the media access control (MAC) address of a router rather than the destination host in larger networks.

What Is Network Monitor?

Network Monitor is introduced here to describe how packets can be captured and analyzed. Make sure that students understand the difference between promiscuous mode and non-promiscuous mode. Describe situations in which Network Monitor can be used for troubleshooting.

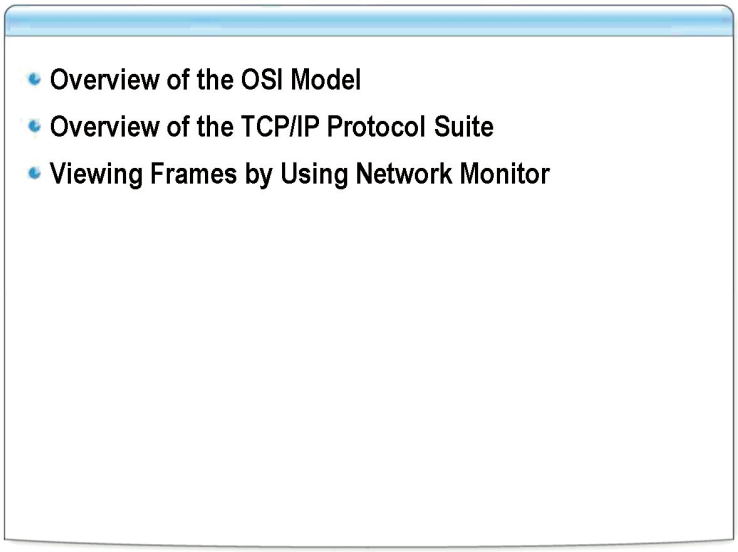
Captured Network Traffic

Describe the information in the Network Monitor Capture Summary window. You might want to capture your own data and use that as an example to explain this topic.

Practice: Viewing Frames by Using Network Monitor

In this practice, students install Network Monitor, capture frames, and then examine the frames. Many students will not have used Network Monitor before. Be sure to actively help them to understand the information that they see. It is important that students understand how to use Network Monitor because it is used in future labs.

Overview



Introduction

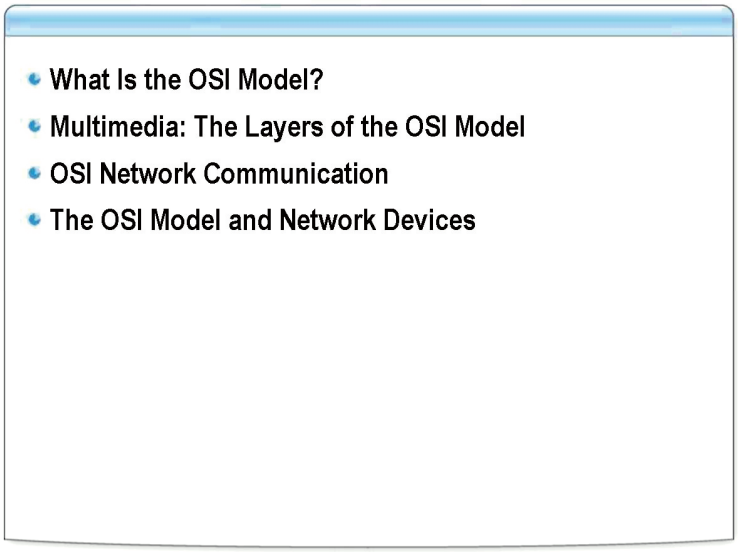
This module provides you with a review of the Open Systems Interconnection (OSI) reference model and the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. Understanding the protocols in the TCP/IP protocol suite enables you to determine whether a host on a network running Microsoft® Windows Server™ 2003 can communicate with other hosts in the network. Knowing the function of each protocol in the TCP/IP protocol suite and how the protocols relate to each other and to the OSI model provides you with the fundamental knowledge to perform common network administration tasks.

Objectives

After completing this module, you will be able to:

- Describe the architecture of the OSI model and the function of each layer.
- Describe the four layers of the TCP/IP suite.
- Capture and view frames by using Network Monitor.

Lesson: Overview of the OSI Model



Introduction

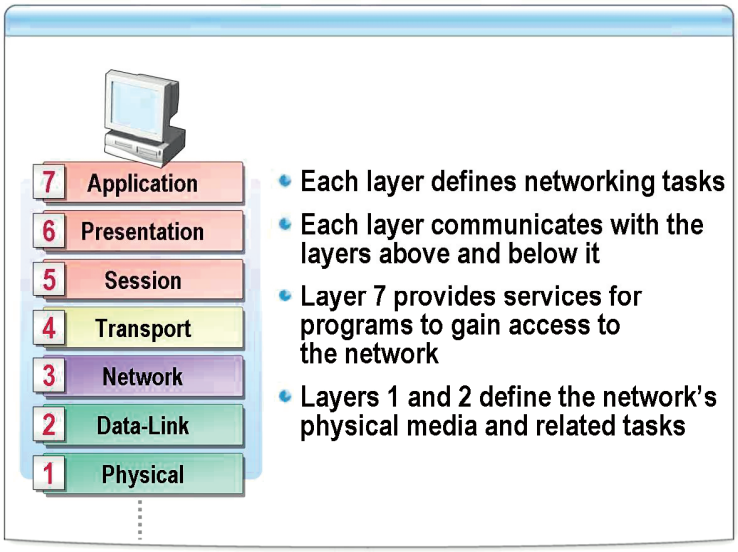
To understand how the protocols in the TCP/IP protocol suite enable network communication, you must understand the concepts behind network communication. The OSI model is a conceptual model that is commonly used as a reference for understanding network communication.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the architecture of the OSI model.
- Describe the function of each layer of the OSI model.
- Explain how data moves across a network by using the OSI model.
- Describe how the functionality of network devices relates to the OSI model.

What Is the OSI Model?



Definition

The OSI model is an architectural model that represents networking communications. It was introduced in 1978 by the International Organization for Standardization (ISO) to standardize the levels of services and types of interactions for computers communicating over a network.

What does the OSI model do?

The OSI model defines the generic tasks that are performed for network communication. You can think of each layer of the OSI model as a piece of software that performs specific tasks for that layer. Each layer communicates with the layer below and the layer above. Data that is transmitted over the network must pass through all seven layers.

How to use the OSI model

The OSI model is used as a common reference point when comparing the function of different protocols and types of network hardware. Understanding the OSI model is important for comparing different products. For example, many switch vendors will refer to their products as layer-2 switches or layer-3 switches. The layers to which they refer are the layers of the OSI model.

Note For more information about the ISO, see the International Organization for Standardization Web site.

The architecture of the OSI model

The OSI model divides network communications into seven layers. Each layer has a defined networking function, as described in the following table.

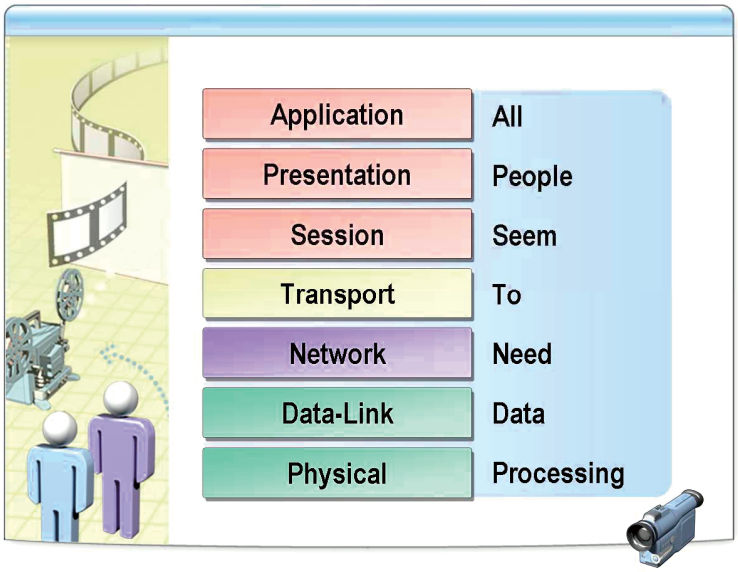
Layer	Function
Application	Layer 7. Provides an entrance point for programs such as Web browsers and e-mail systems to gain access to network services. This layer does not represent programs such as Microsoft Office Word or Microsoft Office Excel®. This layer represents application programming interfaces (APIs) that developers can use to perform network functions when building applications.

(*continued*)

Layer	Function
Presentation	Layer 6. Translates data between different computing systems on a network. The presentation layer translates the data generated by the application layer from its own syntax into a common transport syntax suitable for transmission over a network. When the data arrives at the receiving computer, the presentation layer on the receiving computer translates the syntax into the computer's own syntax.
Session	Layer 5. Enables two applications to create a persistent communication connection. This layer ensures that both the sender and the receiver are ready to communicate. The session layer can also set checkpoints in the communication process to ensure that it can be restarted if communication is interrupted.
Transport	Layer 4. Ensures that packets are delivered in the order in which they are sent and without loss or duplication. On the sending side, this layer is responsible for breaking down larger messages into smaller packets for transmission on the network. On the receiving side, this layer is responsible for reassembling the packets into a single message to pass up to the session layer. In the context of the OSI reference model, a *packet* is an electronic envelope containing information formed from the session layer to the physical layer of the OSI model.
Network	Layer 3. Determines the physical path of the data to be transmitted based on the network conditions, the priority of service, and other factors. This is the only layer of the OSI model that uses logical networking and can move packets between different networks.
Data-link	Layer 2. Provides error-free transfer of data frames from one computer to another over the physical layer. The media access control (MAC) address of a network card exists at this layer and is added to the packet to create a frame. In the context of the OSI reference model, a *frame* is an electronic envelope of information that includes the packet and other information that is added by the seven layers of the OSI model. The data-link layer is responsible for determining when the frame will be sent on the network and then passing the data to the physical layer. Data is passed from the data-link layer to the physical layer as a stream of 1s and 0s.
Physical	Layer 1. Establishes the physical interface and mechanisms for placing a raw stream of data bits on the network cabling. As each bit of information is received from the data-link layer, the physical layer converts it to an appropriate format and transmits it on the network. On a wired network, each bit is translated into an electrical signal. On a fiber optic network, each bit is translated into a light signal.

Note Protocols operating at different layers of the OSI model use different names for the units of data that they create. At the data-link layer, the term *frame* is used. At the network layer, the term *datagram* is used. The more generic term *packet* is used to describe the unit of data created at any layer of the OSI model.

Multimedia: The Layers of the OSI Model



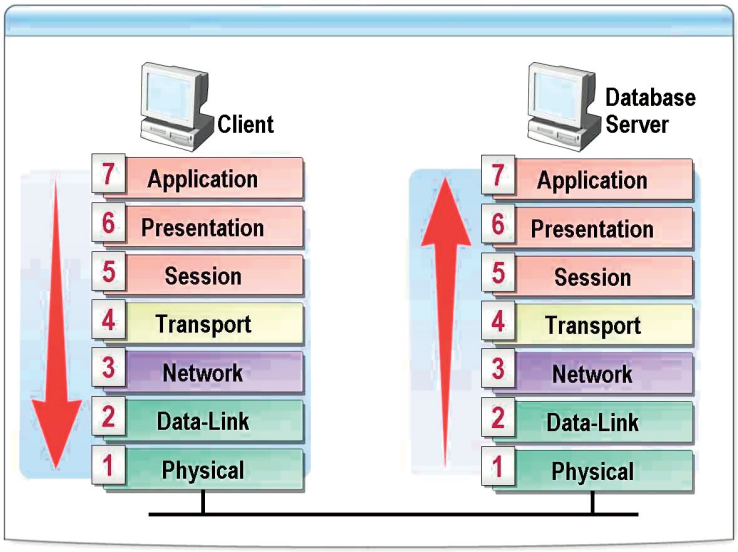
File location

To view the multimedia presentation, *The Layers of the OSI Model*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objective

At the end of this presentation, you will be able to name the OSI layers in order and describe each layer's functionality.

OSI Network Communication



Introduction

To further understand what occurs at each layer of the OSI model, it is useful to look at a specific example of network communication using the OSI model. The following example is for a client/server application. The sender is the client, and the receiver is the database server.

The sending process

The sending process prepares and transmits data over the network as seen in the following table.

Layer	Function
Application	The application layer of the OSI model receives data from the client-side application and passes it to the presentation layer.
Presentation	The presentation layer performs any necessary formatting for the data to be placed on the network. Formatting can include encryption or compression. In this example, the data is compressed.
Session	The session layer confirms that the destination computer is ready to receive data. A connection to the destination is created.
Transport	The transport layer breaks the data into smaller packets for transmission on the network. The packets are also labeled so that they can put back together in their proper order at the destination.
Network	The network layer adds logical addressing information to each packet to ensure that the packets arrive at the correct location.

(*continued*)

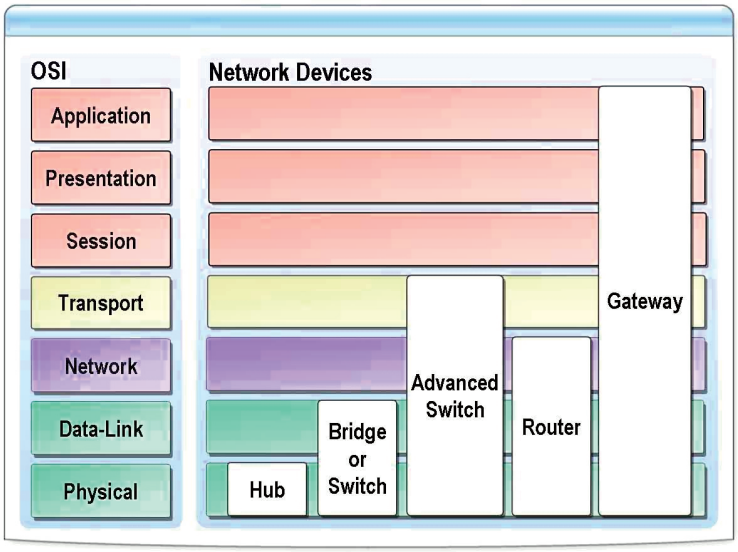
Layer	Function
Data-link	The data-link layer adds physical address information to the packets. The data-link layer also adds a cyclical redundancy check (CRC) to each packet. The CRC is a checksum used ensure that there are no errors in delivery. In addition, the data-link layer monitors the network and determines when it is appropriate to send data. The data is converted to a stream of 1s and 0s and passed to the physical layer.
Physical	As each bit of information is received from the data-link layer, the physical layer converts it to an appropriate format and transmits it on the network. On a wired network, each bit is translated into an electrical signal. On a fiber optic network, each bit is translated into a light signal.

The receiving process

The receiving process accepts incoming signals from the network, converts them to data, and passes the data to an application. In this example, the application is a database. The process is shown in the following table.

Layer	Function
Physical	The physical layer receives electrical signals or light signals from the cabling and converts the signals to 1s and 0s. Each bit is then passed to the data-link layer.
Data-link	The data-link layer organizes the bits into frames. The CRC on each frame is verified to ensure that there were no errors in delivery. If there were errors, the data-link layer requests that the packet be resent. After the CRC is verified, it is removed from the packet. In addition, the data-link layer verifies that the physical address is the receiving computer. If it is, the physical address information is removed from each packet, and the packets are passed to the network layer. If the physical address is not the receiving computer, the packet is dropped.
Network	The network layer confirms that the logical address is the receiving computer. If it is, the logical address information is removed from the packets, and they are passed to the transport layer. If the logical address is not the receiving computer, the packet is dropped.
Transport	The transport layer organizes all the packets back into a single chunk of data and passes the data to the session layer.
Session	When the data transmission is complete, the session layer closes the connection between the sender and receiver.
Presentation	The presentation layer undoes the formatting performed by the sender. In this case, the data is uncompressed and passed to the application layer.
Application	The application layer receives data from the presentation layer and passes it to the appropriate application or service. In this case, the data is passed to the database service running on the server.

The OSI Model and Network Devices



Introduction

One of the common uses of the OSI model is comparing the function of different network devices such as hubs, bridges, switches, routers, and gateways. If you understand the OSI model, you will understand how these devices operate differently and the benefits of each device.

Hubs

Hubs operate at the physical layer (layer 1) of the OSI model. As a result, hubs can only perform tasks with the electrical signal on the network cabling. Hubs regenerate 1s and 0s on network cabling. This allows the signals to be transmitted farther than would be possible without a hub.

Hubs are unable to make decisions about where the regenerated signal should be sent because they function only at the physical layer of the OSI model. Hubs send the regenerated signal out to all ports except the port on which the signal was received.

Note Repeaters have the same function as hubs. The term *multiport repeater* is sometimes used instead of *hub*.

Bridges

Bridges operate at the data-link layer (layer 2) of the OSI model. Bridges are able to control network traffic based on MAC addresses. This is useful for limiting traffic across small wide-area networks (WANs).

In a network with two locations, a bridge is used to separate the two locations and controls the packets transmitted between the two locations. The bridges automatically determine the location of computers by monitoring packets on the network and looking at the source MAC address in the packets. After the bridges have determined the location of the computers, they prevent local network traffic from being transmitted over the WAN.

Bridges are most often used over wireless links between buildings or locations.

Switches

The earliest switches and today's cheaper switches have the same functionality as a bridge and operate at the data-link layer of the OSI model. This functionality allows switches to control network traffic based on MAC addresses. Over time, switches create a table that lists the port location of each computer and direct packets to only the destination computer. This is in contrast to a hub, which propagates packets to all computers on the network. Directing the packets to the proper destination reduces the overall load on the network.

Many midrange and enterprise-level switches now have functionality that extends to layer 3 or layer 4 of the OSI model. Layer-3 switches can perform routing functions similar to a router. Layer-4 switches are application-aware and can give packets different priority levels based on the application that generated the packet.

Routers

Routers operate at the network layer (layer 3) of the OSI model. They are capable of moving packets from one logical network to another. This capability is required for larger local area networks (LANs) and WANs.

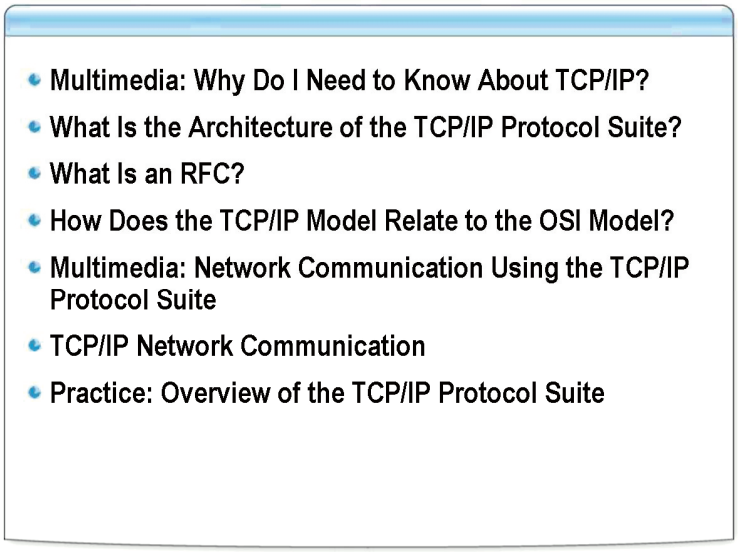
Large networks are sometimes divided into separate smaller networks to control communications between computers. An example of this would be a company with several different departments. Each department would have a small network that was a part of the larger company network. A router would be required to move packets from a computer in one department to a computer in a different department.

Gateways

A gateway is a device that converts one protocol to another. A gateway can operate at any layer of the OSI model, depending on which protocol is being converted.

One of the common gateway types in large organizations is a Systems Network Architecture (SNA) gateway. SNA is a protocol used for communication with mainframe computers. An SNA gateway allows computers on a TCP/IP network to communicate with mainframes by translating the TCP/IP communication into SNA communications. This is required to allow current computers to access older applications running on the mainframe.

Lesson: Overview of the TCP/IP Protocol Suite



Introduction

The protocols in the TCP/IP protocol suite enable computers using different hardware and software to communicate over a network. TCP/IP for Windows Server 2003 provides a standard, routable, enterprise networking protocol to enable users to gain access to the World Wide Web and to send and receive e-mail. This lesson describes the four-layer conceptual model of the TCP/IP suite of protocols and how it maps to the OSI model. In addition, the lesson includes a depiction of a packet moving through the TCP/IP layers.

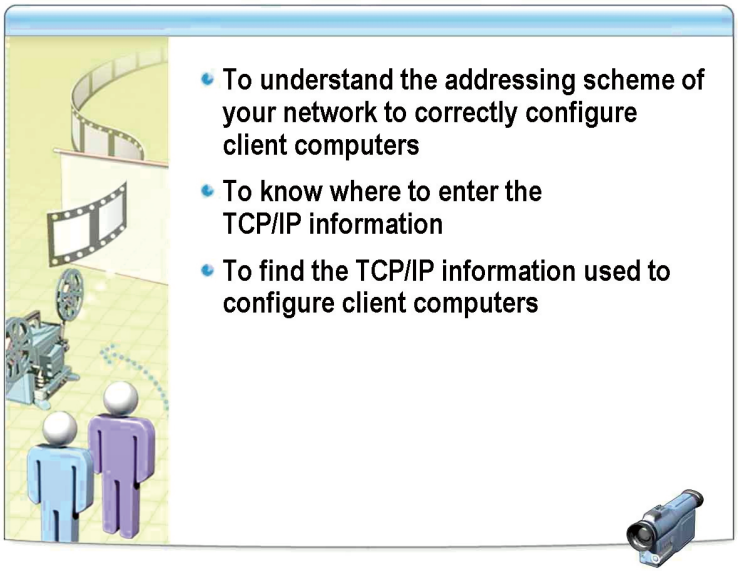
Note For more information about the TCP/IP protocol suite, see RFC 1180 under **Additional Reading** on the Student Materials compact disc.

Lesson objectives

After completing this lesson, you will be able to:

- Recognize why TCP/IP is important.
- Describe the architecture of the TCP/IP protocol suite.
- Describe what an RFC is.
- Associate the protocols of the TCP/IP protocol suite with those of the OSI model.
- Describe the function of the protocols at each layer of the TCP/IP protocol suite.
- Explain how data moves across a network by using the TCP/IP protocol suite.
- Match protocols to the layers of the TCP/IP protocol suite.

Multimedia: Why Do I Need to Know About TCP/IP?



**********ILLEGAL FOR NON-TRAINER USE**********

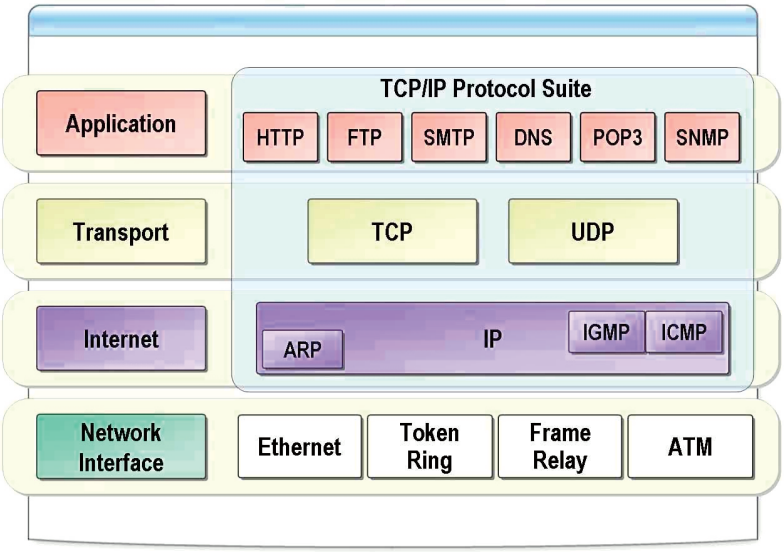
File location

To view the multimedia presentation *Why Do I Need to Know About TCP/IP?*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objective

After you have completed this presentation, you will be able to explain the importance of understanding client computer addressing schemes and where to configure TCP/IP options on a client computer running a Microsoft Windows® operating system.

What Is the Architecture of the TCP/IP Protocol Suite?



Introduction

TCP/IP is an industry-standard suite of protocols that provides communication in a heterogeneous environment. The tasks that are involved in using TCP/IP in the communication process are distributed between protocols that are organized into four distinct layers of the TCP/IP stack.

Four layers of the TCP/IP stack

The four layers of the TCP/IP protocol stack are:

- The application layer.
- The transport layer.
- The Internet layer.
- The network interface layer.

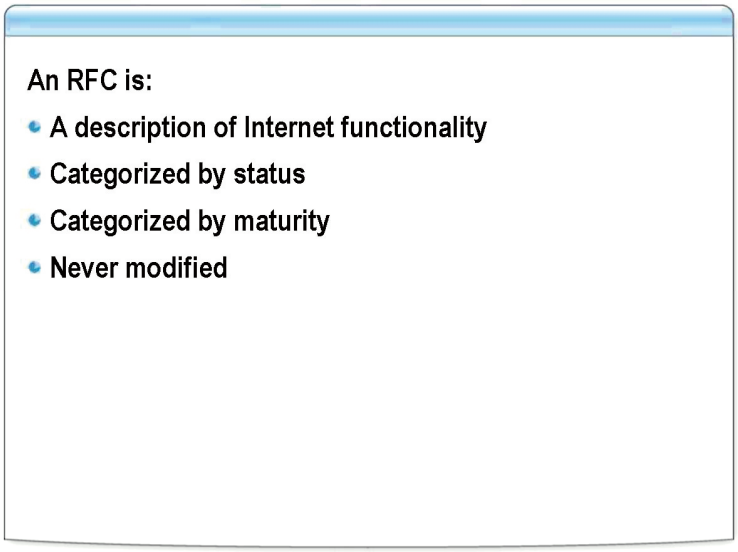
Benefits of TCP/IP

Dividing the network functions into a stack of separate protocols, rather than creating a single protocol, provides several benefits:

- Separate protocols make it easier to support a variety of computing platforms. Creating or modifying protocols to support new standards does not require modification of the entire protocol stack.
- Having multiple protocols operating at the same layer makes it possible for applications to select the protocols that provide only the level of service required.
- Because the stack is split into layers, the development of the various protocols can proceed simultaneously, using personnel who are uniquely qualified in the operations of the particular layers.

Note For more information about the TCP/IP application layer and support protocols, see RFC 1123 under **Additional Reading** on the Student Materials compact disc. For more information about the transport, Internet, and network interface layers, see RFC 1122 under **Additional Reading** on the Student Materials compact disc.

What Is an RFC?



Definition

The standards for TCP/IP are published in a series of documents called requests for comments (RFCs). RFCs describe the internal workings of the Internet. Some RFCs describe network services or protocols and their implementations, whereas others summarize policies. TCP/IP standards are always published as RFCs, although not all RFCs specify standards.

RFC status

TCP/IP standards are not developed by a committee, but rather by consensus. Anyone can submit a document for publication as an RFC. Documents are reviewed by a technical expert, a task force, or the RFC editor and are then assigned a status. The status specifies whether a document is being considered as a standard. The various status levels are listed in the following table.

Status	Description
Required	Must be implemented on all TCP/IP-based hosts and gateways.
Recommended	Encouraged that all TCP/IP-based hosts and gateways implement the RFC specification. Recommended RFCs are usually implemented.
Elective	Implementation is optional. Its application has been agreed to but is not a requirement
Limited Use	Not intended for general use.
Not Recommended	Not recommended for implementation.

RFC maturity

If a document is being considered as a standard, it goes through stages of development, testing, and acceptance known as the *Internet Standards process*. These stages, which are formally labeled *maturity levels*, are applied in addition to the RFC status. The possible maturity levels are listed in the following table.

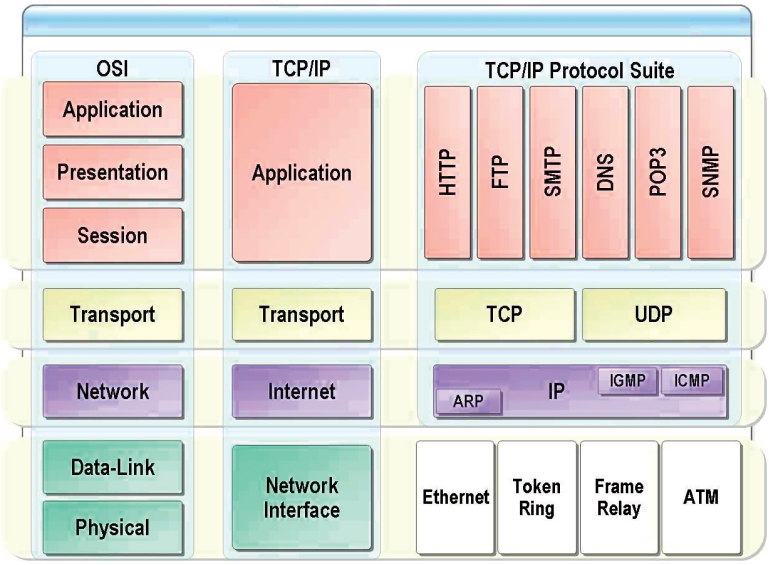
Maturity level	Description
Proposed Standard	A Proposed Standard specification is generally stable, has resolved known design choices, is believed to be well understood, has received significant community review, and appears to enjoy enough community interest to be considered valuable.
Draft Standard	A Draft Standard must be well understood and known to be quite stable, both in its semantics and as a basis for developing an implementation.
Internet Standard	The Internet Standard specification (which might simply be referred to as a Standard) is characterized by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefit to the Internet community.

RFC numbers

When a document is published, it is assigned an RFC number. The original RFC is never updated. Each time an RFC is revised and moves through the maturity levels, a new RFC is published with a new number. Therefore, it is important to verify that you have the most recent RFC on a particular topic.

Note More information about RFCs, including a complete list of RFCs, can be found at the IETF Web site. Also, RFC 2026 contains detailed information about the RFC approval process.

How Does the TCP/IP Model Relate to the OSI Model?



Introduction

The OSI model defines distinct layers related to packaging, sending, and receiving data transmissions in a network. The layered suite of protocols that form the TCP/IP stack carry out these functions.

Application layer

The application layer corresponds to the application, presentation, and session layers of the OSI model. This layer provides services and utilities that enable applications to access network resources.

On a computer running Windows Server, applications can request network services by using Windows Sockets or network basic input/output systems (NetBIOS). Windows Sockets is used by Internet applications and most other applications. NetBIOS is used for file sharing by clients running Microsoft Windows 98 and earlier, and by many older Windows applications. The developer of the application specifies whether an application will use Windows Sockets or NetBIOS.

Some application-layer protocols are described in the following table.

Protocol	Description
HTTP	Hypertext Transfer Protocol. Specifies the client/server interaction processes between Web browsers and Web servers.
FTP	File Transfer Protocol. Performs file transfers and basic file management tasks on remote computers.
SMTP	Simple Mail Transfer Protocol. Carries e-mail messages between servers and from clients to servers.
DNS	Domain Name System. Resolves Internet host names to IP addresses for network communications.
POP3	Post Office Protocol version 3. Used by mail clients for reading e-mail.
SNMP	Simple Network Management Protocol. Enables you to collect information about network devices such as hubs, routers, and bridges. Each piece of information to be collected about a device is defined in a Management Information Base (MIB).

Transport layer

The transport layer corresponds to the transport layer of the OSI model and is responsible for guaranteed delivery and end-to-end communication using one of two protocols described in the following table.

Protocol	Description
TCP	Transmission Control Protocol. Provides connection-oriented reliable communications for applications. Connection-oriented communication confirms that the destination is ready to receive data before sending. TCP confirms that all packets are received to make communication reliable. Reliable communication is desired in most cases and is used by most applications. Web servers, FTP clients, and other applications that move large amounts of data use TCP.
UDP	User Datagram Protocol. Provides connectionless and unreliable communication. Reliable delivery is the responsibility of the application when UDP is used. Applications use UDP for faster communication with less overhead than TCP. Applications such as streaming audio and video use UDP so that a single missing packet will not delay playback. UDP is also used by applications that send small amounts of data, such as DNS name lookups.

Internet layer

The Internet layer corresponds to the network layer of the OSI model. The protocols at this layer encapsulate transport-layer data into units called *datagrams*, address them, and route them to their destinations.

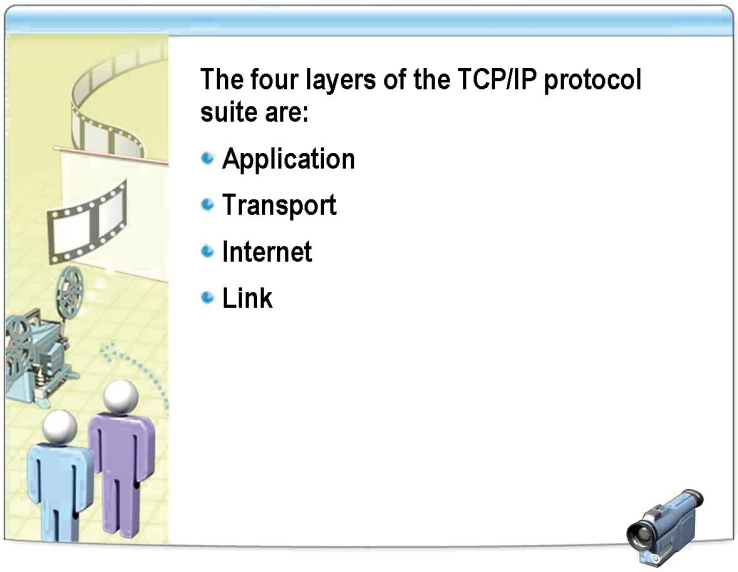
There are four protocols at the Internet layer, as described in the following table.

Protocol	Description
IP	Internet Protocol. Addresses and routes packets between hosts and networks.
ARP	Address Resolution Protocol. Obtains hardware addresses of hosts located on the same physical network.
IGMP	Internet Group Management Protocol. Manages host membership in IP multicast groups.
ICMP	Internet Control Message Protocol. Sends messages and reports errors regarding the delivery of a packet.

Network interface layer

The network interface layer (sometimes referred to as the link layer or data-link layer) corresponds to the data-link and physical layers of the OSI model. This layer specifies the requirements for sending and receiving packets on the network media. This layer is often not formally considered part of the TCP/IP protocol suite because the tasks are performed by the combination of the network card driver and the network card.

Multimedia: Network Communication Using the TCP/IP Protocol Suite



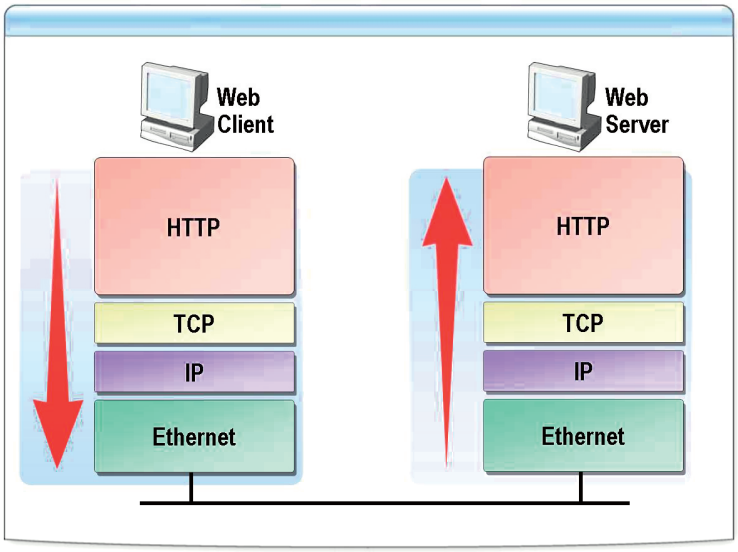
File location

To view the multimedia presentation *Network Communication Using the TCP/IP Protocol Suite*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objective

After completing this presentation, you will be able to explain the role of each layer in the TCP/IP protocol stack and how an IP packet is sent and received by each layer.

TCP/IP Network Communication



Introduction

To further understand what occurs at each layer of the TCP/IP protocol suite, it is useful to look at a specific example of network communication using the TCP/IP protocol suite. The following example is for a Web client communicating with a Web server.

The sending process

The sending process prepares and transmits data over the network, as described in the following table.

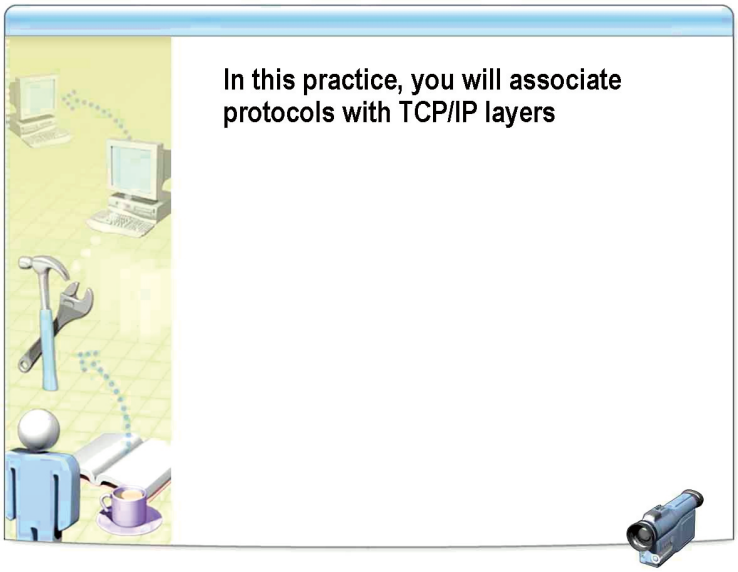
Layer	Function
Application	The Web browser software uses HTTP to build a request for the Web server and passes the request to TCP.
Transport	TCP initiates a session with the Web server that confirms details such as maximum packet size. If the request is large enough, TCP will also break the request into multiple packets. Packets are passed to IP.
Network	IP adds the source and destination IP addresses to the packets and passes them to the network card driver.
Network interface	Ethernet is a combination of functionality in the network card driver and the network card hardware. It is responsible for adding a source and destination MAC address and a CRC check to the packets. Ethernet is also responsible for placing the packets on the network media for delivery to the destination Web server.

The receiving process

The receiving process accepts data from the network and passes it to the Web server, as described in the following table.

Layer	Function
Network interface	Ethernet receives the signals from the network and converts them to a frame, and the CRC check on the frame is verified. The destination MAC addresses on the packets are verified, and the packets are passed up to IP.
Network	IP verifies the destination IP address and passes the packets to TCP.
Transport	TCP confirms that all of the packets have arrived and recombines them into a single request. TCP then passes the request to HTTP. The session initiated by TCP on the client side stays open until the entire communication process is complete.
Application	HTTP is used by the Web server to interpret the request. The Web server then sends a response back to the Web client. This response is typically the contents of a Web page, but it can also be an error message.

Practice: Overview of the TCP/IP Protocol Suite



Objectives

In this practice, you will associate protocols with TCP/IP layers.

Instructions

No virtual machines are required for this practice.

Practice

► **Associate protocols with TCP/IP layers**

1. Insert the Student Materials compact disc.
2. If necessary, click **Start**, click **Run**, type ***X*:\StartCD.exe**, and then click **OK**.

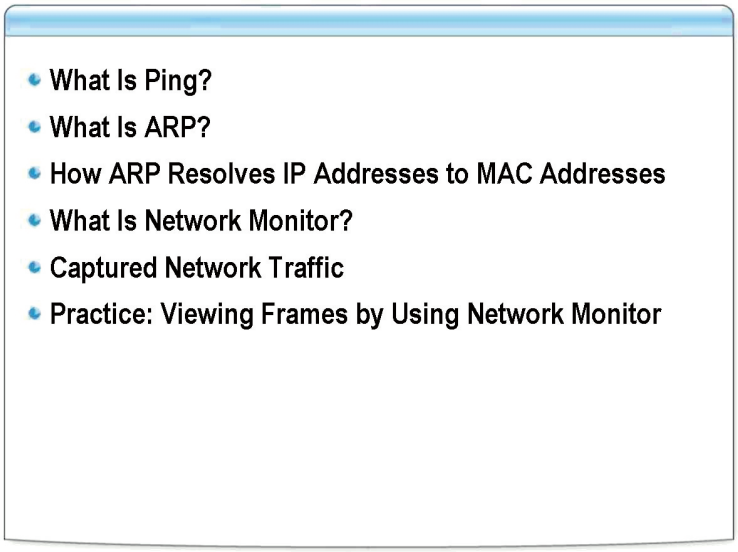
> **Note** *X* represents the drive where the Student CD is located.

3. Click **Yes** to allow active content.
4. Click **Multimedia**.
5. Under **Module 1: Reviewing the Suite of TCP/IP Protocols**, click **Practice: Associating Protocols of an IP Address**.

► **Prepare for the next practice**

1. Start the DEN-DC1 virtual machine.
2. Start the DEN-SRV1 virtual machine.
3. Start the DEN-CL1 virtual machine.

Lesson: Viewing Frames by Using Network Monitor



Introduction

Microsoft Network Monitor is a protocol analyzer that you can use to analyze and monitor network communications. Network Monitor simplifies your task of isolating complex network problems by performing real-time network traffic analysis and capturing packets for decoding and analysis.

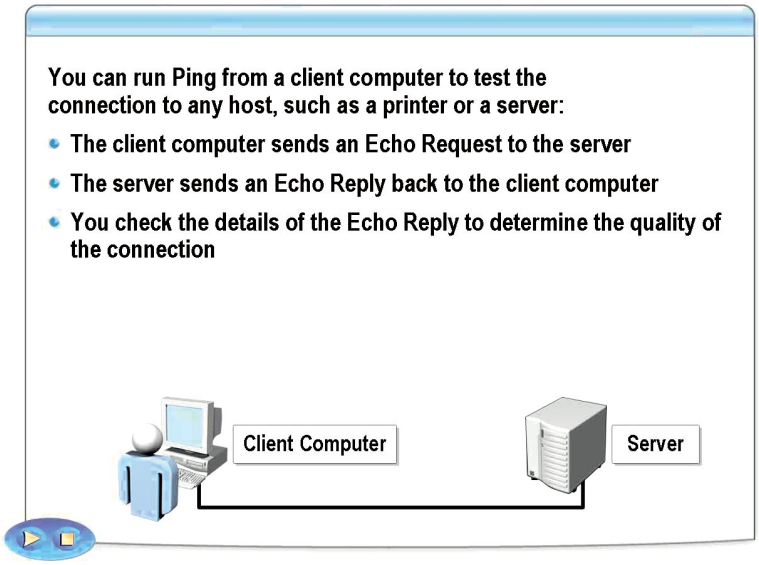
In this lesson, you will use the Ping utility (Ping) to generate traffic for analysis.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the Ping utility.
- Describe ARP.
- Describe how ARP resolves IP addresses to MAC addresses.
- Describe Network Monitor.
- Describe captured network traffic.
- View frames by using Network Monitor.

What Is Ping?



Definition

TCP/IP implementations include a basic network utility named Ping. You use Ping to test whether a target computer's networking hardware and protocols are functioning correctly, at least up to the network layer of the OSI model. When you use Ping, you generate network traffic. You can then use Network Monitor to analyze this traffic.

Example of using Ping

You run Ping by using the syntax ping *target*, where *target* is the computer name or IP address of the target computer. For example, in the slide:

1. The client computer is running the **ping** command, specifying the server as the target computer.
2. Ping generates a series of Echo messages using ICMP and transmits the Echo messages to the server.
3. The server sends Echo Reply messages back to the client computer.
4. When the originating computer receives the Echo Reply messages, it produces output.

Example of Ping output

When the originating computer receives the Echo Reply messages from the target computer, it produces a display similar to the following:

```
Pinging DEN-DC1 (10.10.0.2) with 32 bytes of data:
Reply from 10.10.0.2: bytes=32 time<10ms TTL=128
Reply from 10.10.0.2: bytes=32 time<10ms TTL=128
Reply from 10.10.0.2: bytes=32 time<10ms TTL=128
Reply from 10.10.0.2: bytes=32 time<10ms TTL=128
Ping statistics for 10.10.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

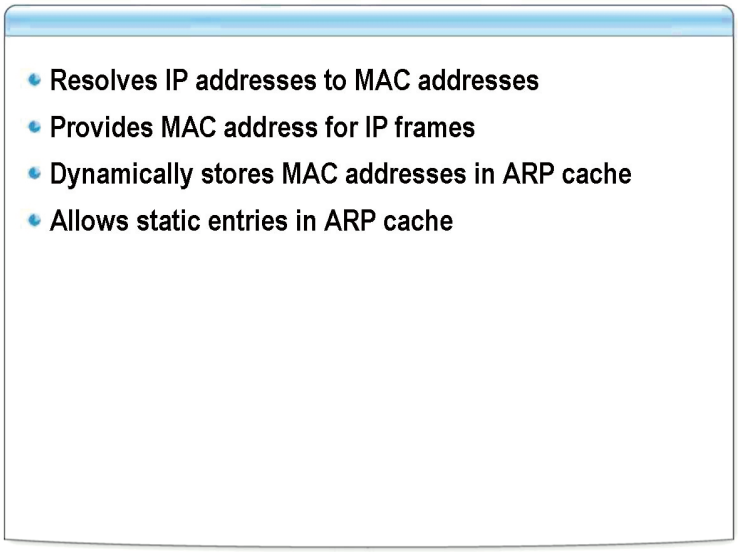
This display shows the echo replies from the target computer. Information displayed includes the IP address of the target computer, the number of bytes of data included with each request, the elapsed time between the transmission of each request and the receipt of each reply, and the value of the Time to Live (TTL) field in the IP header. In this particular example, the target computer is on the same LAN, so the time measurement is very short—less than 10 milliseconds.

Responses to Ping requests

When you submit a Ping request to, or *ping*, a computer on the Internet, the interval is likely to be longer than when you ping a computer on your local network. A reply from the target computer indicates that its networking hardware and protocols are functioning correctly, at least as high as the network layer of the OSI model. Be careful not to assume that simply because a host did not respond to an echo request it is offline or that you are not properly connected to the network. Inability to obtain a reply to a ping can be an indication of network trouble.

Note Because of security issues such as the Ping of Death, in which a remote host sends an oversized packet to interrupt service in another system or to prevent outsiders from gaining network configuration information, it is not uncommon for network administrators to prevent external systems from responding to a Ping request.

What Is ARP?



Definition

The destination MAC address in an IP frame is critical to the proper delivery of IP frames on a network. ARP is used to resolve IP addresses to MAC addresses. A MAC address is a 6-byte (48-bit) number that is used to uniquely identify network devices. The MAC address for a network card or network device is configured by the manufacturer of the device. The conversion of IP addresses to MAC addresses is done by computers as IP frames are built.

Why is ARP required?

When IP frames are delivered on a network, the network cards and network devices use MAC addresses to filter out packets that are not addressed to them. When an IP frame is received by a network card, the network card will verify whether the destination MAC address in the frame matches the MAC address of the network card. If the destination MAC address in the frame matches the MAC address of the network card, the frame is accepted and passed up to the IP. However, if the destination MAC address does not match the MAC address of the network card, the IP frame is dropped.

Note Some network cards support *promiscuous mode*. A network card that is placed in promiscuous mode does not filter packets based on the destination MAC address and will accept all packets that are received. This mode is used by network-sniffing software such as Network Monitor.

The ARP cache

To minimize the amount of broadcast network traffic that ARP generates, the computer stores recently resolved IP addresses and their corresponding MAC addresses in a cache. Entries automatically added to the ARP are called *dynamic entries*. TCP/IP checks the cache before sending out a broadcast request to obtain a MAC address.

Dynamic entries in the ARP cache have a time-out value of two minutes. If a dynamic ARP cache entry is not used within two minutes, it is removed from the ARP cache. If a dynamic ARP cache entry is used within two minutes, the time-out for the entry is increased to 10 minutes.

Static cache entries

You can place static entries directly into the ARP cache by using the Arp.exe utility. However, this is not recommended, as it will cause problems when IP addresses are changed or a network card is replaced. The amount of network traffic generated by ARP requests is unlikely to degrade network performance.

Note Static entries in the ARP cache are erased when the system is restarted.

How to use ARP to isolate connection issues

You can use the ARP tool to isolate connection issues. For example, if two computers on the same subnet cannot communicate with each other, you can use ARP to determine whether the correct MAC addresses are listed. To verify that the MAC addresses are correctly listed in the ARP cache, you run the **arp -a** command on each computer. This displays the IP and MAC addresses listed in the ARP cache for each computer. You verify that the MAC address listed in the ARP cache is the same as the actual MAC address for the destination computer by using Ipconfig.exe.

Example of output from the arp –a command

The following example shows the output for the **arp -a** command, which displays the ARP cache tables for all network interfaces:

```
C:\>arp -a
Interface: 10.10.0.2 ---  0x2
Internet address   Physical address     Type
10.10.0.1          00-e0-34-c0-a1-40    dynamic
10.10.1.231        00-00-f8-03-6d-65    dynamic
10.10.3.34         08-00-09-dc-82-4a    dynamic
10.10.4.53         00-c0-4f-79-49-2b    dynamic
10.10.5.102        00-00-f8-03-6c-30    dynamic
```

ARP syntax and parameters

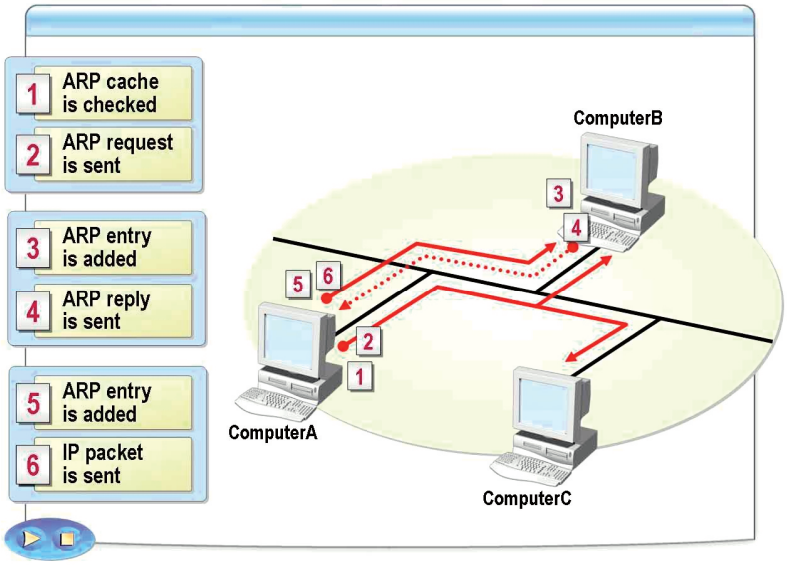
ARP uses the following syntax:

arp [**-a** [*InetAddr*] [**-N** [*IfaceAddr*]] [**-g** [*InetAddr*] [**-N** [*IfaceAddr*]] [**-d** *InetAddr* [*IfaceAddr*]] [**-s** *InetAddr EtherAddr* [*IfaceAddr*]]

The following table describes the function of the ARP parameters.

Parameter	Function
-a	Displays current ARP cache entries for all interfaces. To display the ARP cache entry for a specific IP address, type **arp -a** *InetAddr*, where *InetAddr* is an IP address.
-N	Lists ARP entries for the interface specified by **-N** *IfaceAddr*, where *IfaceAddr* is the IP address assigned to the interface. The **-N** parameter is case-sensitive.
-g	Same as **-a**.
-d	Removes an entry specified by its IP address (*InetAddr*) from the ARP cache. To remove an entry for a specific interface, type **arp -d** *IfaceAddr*, where *IfaceAddr* is the IP address assigned to that interface. To delete all entries, use the asterisk (*) wildcard in place of *InetAddr*.
-s	Adds a static entry to the ARP cache that resolves the specified IP address (*InetAddr*) to the MAC address (*EtherAddr*). To add a static ARP cache entry to the table for a specific interface, type **arp -s** *IfaceAddr*, where *IfaceAddr* is the IP address assigned to that interface.
/?	Displays ARP parameters.

How ARP Resolves IP Addresses to MAC Addresses



Introduction

Before transmitting an IP packet, TCP/IP clients must resolve the forwarding, or next-hop, IP address to its corresponding MAC address. If the MAC address for the next-hop is not in the ARP cache, the client will broadcast an ARP request frame to obtain the MAC address. The computer using that IP address responds with an ARP reply message containing its MAC address. With the information in the reply message, the computer can encapsulate the IP packet in the appropriate frame and transmit it to the next-hop.

The ARP process

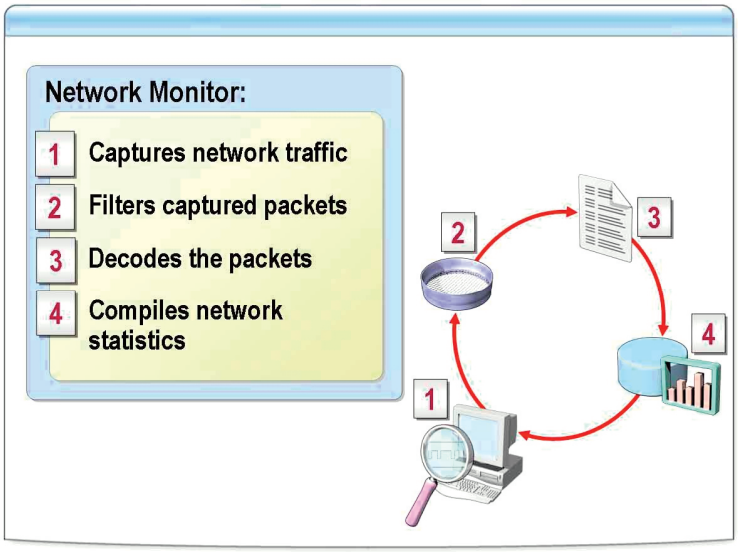
In the preceding illustration, ComputerA is broadcasting an ARP request to ComputerB and ComputerC. The following steps describe the process:

1. On ComputerA, ARP consults its own ARP cache for an entry for the destination IP address. If an entry is found, ARP proceeds to step 6.
2. If an entry is not found, ARP on ComputerA builds an ARP request frame containing its own MAC address and IP address and the destination IP address. ARP then broadcasts the ARP request.
3. ComputerB and ComputerC receive the broadcasted frame and the ARP request is processed. If the receiving computer's IP address matches the requested IP address (the destination IP address), its ARP cache is updated with the address of the sender of the ARP request, ComputerA.

   If the receiving host's IP address does not match the requested IP address, as in the case of ComputerC, the ARP request is discarded.
4. ComputerB formulates an ARP reply containing its own MAC address and sends it directly to ComputerA.
5. When ComputerA receives the ARP reply from ComputerB, it updates its ARP cache with the IP address and MAC address.

   ComputerA and ComputerB now have each other's IP to MAC address mappings in their ARP caches.
6. ComputerA sends the IP packet to ComputerB.

What Is Network Monitor?



Definition

Network Monitor is a utility included in Windows Server 2003, in Windows 2000 Server products, and in Microsoft Systems Management Server. The version that is included in Windows Server is capable of capturing only network traffic that is addressed to the server. The version of Network Monitor in Microsoft Systems Management Server operates in promiscuous mode and can capture all network traffic.

Uses of Network Monitor

You can use Network Monitor to:

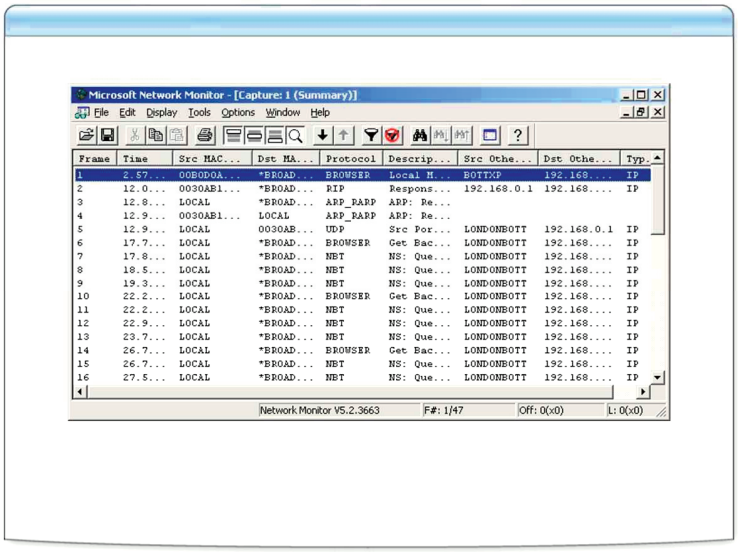
- Locate client-to-server connection problems.
- Identify computers that make a disproportionate number of service requests.
- Capture frames (packets) directly from the network.
- Display and filter captured frames.

How Network Monitor works

To monitor network traffic, Network Monitor:

1. Captures a snapshot of network traffic.
2. Uses filters to select or highlight specific packets.
3. Decodes the packets in a language of the individual protocols.
4. Compiles network statistics.

Captured Network Traffic



**********ILLEGAL FOR NON-TRAINER USE**********

Introduction

When you capture a sample of network traffic, the Network Monitor Capture Summary window displays a chronological list of the frames in your sample.

The following table describes the fields that are displayed for each frame in your sample.

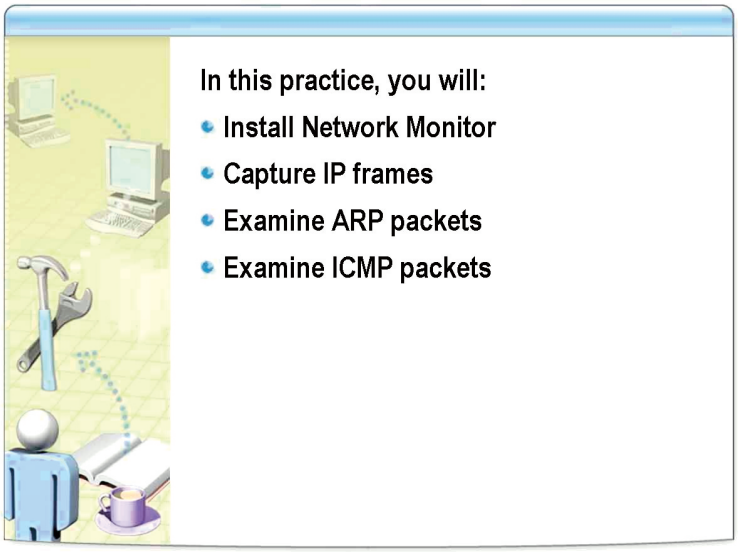
Field	Description
Frame	Shows the number of the frame in the sample.
Time	Indicates the time (in seconds) at which the frame was captured, measured from the beginning of the sample.
Src MAC Addr	Gives the hardware address of the network interface in the computer that transmitted the frame. For computers that the analyzer recognizes by a friendly name, such as a NetBIOS name, this field contains that name instead of the address. The computer on which the analyzer is running is identified as LOCAL.
Dst MAC Addr	Gives the hardware address of the network interface in the computer that received the frame. Friendly names are substituted if available. By compiling an address book of the computers on your network, you can eventually have frame captures that use only friendly names.
Protocol	Shows the dominant protocol in the frame. Each frame contains information generated by protocols running at several different layers of the OSI model.
Description	Indicates the function of the frame, using information specific to the protocol referenced in the Protocol field.
Src Other Addr	Specifies another address used to identify the computer that transmitted the frame.

(*continued*)

Field	Description
Dst Other Addr	Specifies another address (such as an IP address) used to identify the computer that received the frame.
Type Other Addr	Specifies the type of address used in the Src Other Addr and Dst Other Addr fields.

Tip To work with large capture files, increase the size of the Windows page file, and save large capture files before viewing them.

Practice: Viewing Frames by Using Network Monitor



Objectives

In this practice, you will:

- Install Network Monitor.
- Capture IP frames.
- Examine ARP packets.
- Examine ICMP packets.

Instructions

Ensure that the DEN-DC1, DEN-SRV1, and DEN-CL1 virtual machines are running.

Note Microsoft recommends that you log on using a standard user account and use the **Run As** command to perform administrative tasks. In this practice, you will log on as Administrator for convenience.

Practice

► **Install Network Monitor**

1. On DEN-SRV1, log on to the **Contoso** domain as **Administrator**, with a password of **Pa$$w0rd**.
2. Click **Start**, point to **Control Panel**, and then click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. In the **Windows Components Wizard** dialog box, click **Management and Monitoring Tools**, and then click **Details**.
5. Select the check box next to **Network Monitor Tools**, click **OK**, and then click **Next**.
6. Click **Finish**.
7. Close **Add or Remove Programs**.

► **Capture IP frames**

1. On DEN-DC1, log on as **Administrator**, with a password of **Pa$$w0rd**.
2. Click **Start**, point to **Administrative Tools**, and then click **Network Monitor**.
3. Click **OK** to begin selecting the network on which you want to capture data.
4. Expand **Local Computer**, click **Local Area Connection**, and then click **OK**. Maximize the Microsoft Network Monitor window.
5. On DEN-CL1, log on to the **Contoso** domain as **Paul**, with a password of **Pa$$w0rd**.
6. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
7. Type **arp –d *** and then press ENTER to delete all entries in the ARP cache.
8. On DEN-DC1, on the **Capture** menu, click **Start**.
9. On DEN-CL1, type **ping 10.10.0.2**, and then press ENTER.
10. Wait for the **Ping** command to complete on DEN-CL1.
11. On DEN-DC1, on the **Capture** menu, click **Stop**.
12. On the **Capture** menu, click **Display Captured Data**.

► **Examine ARP packets**

1. On DEN-DC1, on the **Display** menu, click **Filter**.
2. Double-click **Protocol==Any**.
3. Click **Disable All**.
4. Under **Disabled Protocols**, double-click **ARP_RARP:** and then click **OK**.
5. Click **OK**. Notice that only two frames are visible now. These are the two ARP packets.
6. Read the description of the two frames that are listed. Notice that the first is an ARP request for the IP address 10.10.0.2 and the second is the ARP reply.
7. Double-click the first frame to display more detailed information about the packet. The middle pane shows the decoded information about the frame. The bottom pane shows the packet displayed as hex values and ASCII.
8. In the middle pane, expand **ARP_RARP: ARP: Request, Target IP: 10.10.0.2** to display detailed information about the ARP request, including the MAC address and IP address of the sender.

► **Examine ICMP packets**

1. On the **Display** menu, click **Disable Filter**.
2. On the **Display** menu, click **Colors**.
3. In the **Protocol Colors** dialog box, click **ICMP**.
4. Under **Colors**, set the foreground to red, and then click **OK**. This displays all ICMP packets in red.
5. Click the first red frame to display the details of the ICMP ECHO from 10.10.0.20 (DEN-CL1) to 10.10.0.2 (DEN-DC1).
6. In the middle pane, expand **FRAME: Base frame properties** to display general information about the frame.
7. Expand **ETHERNET: EType = Internet IP (IPv4)** to display the source and destination MAC addresses.
8. Expand **IP: Protocol = ICMP – Internet Control Message** to display the source and destination IP addresses as well as other IP information.
9. Expand **ICMP: Echo: From 10.10.00.20 to 10.10.00.02** to display detailed information about the ICMP protocol. Notice that the ICMP packet type is **Echo**.
10. Click **ICMP: Packet Type = Echo**. Notice that the hexadecimal value that corresponds to this information is selected in the bottom pane. The hexadecimal value is **08**.
11. In the top pane, click the second red frame.
12. If necessary, in the middle pane, expand **ICMP: Echo Reply: to 10.10.00.20 From 10.10.00.02**. Notice that the packet type is **Echo Reply**.
13. Close Network Monitor. Do not save the frame capture.

Important When you have finished the practice, shut down all the virtual machines without saving changes.
