
Module 1: Reviewing the Suite of TCP/IP Protocols

Contents

Overview	1
Lesson: Overview of the OSI Model	2
Lesson: Overview of the TCP/IP Protocol Suite	7
Lesson: Viewing Frames Using Network Monitor	14



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, Microsoft Press, MSDN, PowerPoint, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Instructor Notes

Presentation:
70 minutes

Lab:
00 minutes

This module provides students with a review of the Open Systems Interconnection (OSI) reference model and the suite of Transmission Control Protocol/Internet Protocol (TCP/IP) protocols. Knowing the function of each of the protocols in the TCP/IP 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 basic architecture of the OSI model and the function of each layer.
- Describe the four layers of the TCP/IP protocol suite.
- Describe how the layers of the TCP/IP model relate to the layers of the OSI model.
- Describe the function of each of the TCP/IP protocols.
- Describe how the TCP/IP protocols relate to each other.
- Install Network Monitor.
- Capture and view packets by using Network Monitor.

Required materials

To teach this module, you need the Microsoft® PowerPoint® file 2276A_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, all the features of the slides may not be displayed correctly.

Preparation tasks

To prepare for this module:

- Read all of the materials for this module.
- Complete the practices.
- Read the referenced Request for Comments (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 fundamental 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 may not be entirely suitable in some places, such as the translation of the document into the recipient's language at the presentation layer.

Practice: Putting the Layers of the OSI model in Order

Ensure that this interactive media piece is not overlooked. The goal of the practice is to give students an opportunity to apply an OSI mnemonic for future reference.

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 may be required to perform as administrators and 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 contained 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 suite, is crucial for their understanding of network communications systems. Tell them that RFC 1180 includes a tutorial that describes the TCP/IP protocol suite.

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: How an IP Packet Moves Through the Suite of TCP/IP Protocols

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.

Practice: Associating the TCP/IP Suite of Protocols with the OSI Model

This practice will reinforce students' ability to associate the TCP/IP suite of protocols with the OSI model.

Lesson: Viewing Frames 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 Network Monitor?

Network Monitor is introduced here to describe how packets can be captured and analyzed. Make sure students understand the difference between promiscuous mode and non-promiscuous mode. Do not spend any time discussing the troubleshooting aspects of this topic.

Practice: Installing Network Monitor

Briefly describe or demonstrate the steps to install Network Monitor, and then have students complete the practice. Students must complete this practice to perform the remaining practices in this module. Students who have completed the prerequisites for this course will be familiar with Run as. For any students who are not familiar with Run as, refer them to Microsoft Windows® Server 2003 Help.

How to Capture Frames

Briefly demonstrate the steps to capture network traffic, and then have the students complete the practice. Suggest that students use Ping to test, or *ping* each other's computers.

Practice: Capturing Frames

Tell students to leave the window open at the completion of this practice in preparation for the next practice.

How to Filter for Select Frames

Briefly demonstrate the steps to filter network traffic, and then have the students complete the practice. Suggest students ping the London computer.

Examining Captured Network Traffic

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

Practice: Examining Packets

To complete this practice, students must have installed Network Monitor in the previous practice. This practice reinforces using Network Monitor and viewing the different protocol packets. Explain the relevance of the packets students are looking at and relate them to the TCP/IP protocols. If time permits, have students expand the packets to view additional data, and show examples of additional protocols. Make sure to go through the questions and answers in this practice.

Customization Information

This section identifies the practice and lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

There are no labs in this module, and as a result, there are no lab setup requirements or configuration changes that affect replication or customization.

Practice or Lab Setup

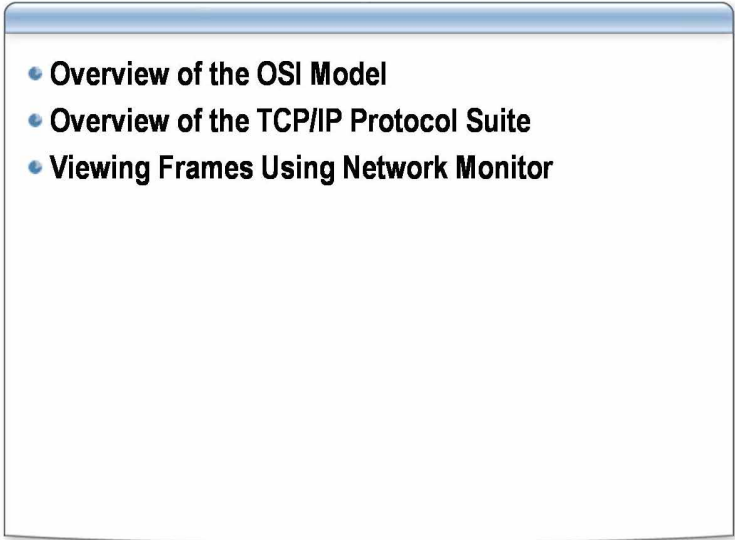
There are no practice setup requirements that affect replication or customization.

Practice Results

There are no configuration changes on student computers that affect replication or customization.

Performing the practices in this module introduces the following configuration change: Microsoft Network Monitor is installed on the student computer.

Overview

- 
- Overview of the OSI Model
 - Overview of the TCP/IP Protocol Suite
 - Viewing Frames Using Network Monitor

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

Introduction

This module provides you with a review of the Open Systems Interconnection (OSI) reference model and the suite of Transmission Control Protocol/Internet Protocol (TCP/IP) protocols. Understanding the protocols in the TCP/IP 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 of the protocols in the TCP/IP 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 basic architecture of the OSI model and the function of each layer.
- Describe the four layers of the TCP/IP protocol suite.
- Describe how the layers of the TCP/IP model relate to the layers of the OSI model.
- Describe the function of each of the TCP/IP protocols.
- Describe how the TCP/IP protocols relate to each other.
- Install Network Monitor.
- Capture and view packets by using Network Monitor.

Lesson: Overview of the OSI Model

- 
- What Is the OSI Model?
 - The Layers of the OSI Model

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

Introduction

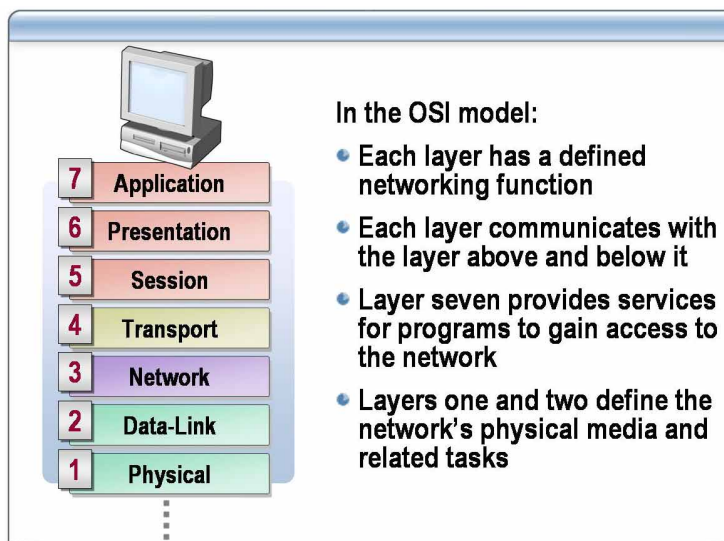
To understand how the TCP/IP protocols enable network communications, you must understand the concepts behind network communications. The OSI model is a conceptual model that is commonly used as a reference for understanding network communications.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the architecture of the OSI model.
- Describe how data moves between the layers of the OSI model.
- Describe the function of each layer of the OSI model.

What Is the OSI Model?



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

Introduction

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

Note For more information about the ISO, see International Organization for Standards, <http://www.iso.ch>.

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.

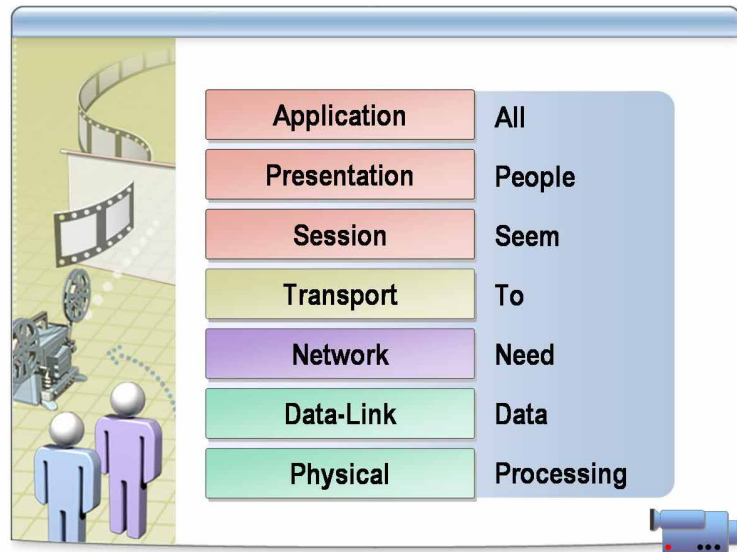
Layer	Function
Application	Layer seven. Provides an entrance point for programs such as Web browsers and e-mail systems to gain access to network services.
Presentation	Layer six. Translates data between different computing systems on a network. The presentation layer translates the data generated by the application layer from its own syntax to 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 five. Enables two applications to create a persistent communication connection.
Transport	Layer four. Ensures that packets are delivered in the order in which they are sent and without loss or duplication. In the context of the OSI reference model, a <i>packet</i> is an electronic envelope containing information formed from the session layer to the physical layer of the OSI model.

(continued)

Layer	Function
Network	Layer three. Determines the physical path of the data to be transmitted based on the network conditions, the priority of service, and other factors.
Data-link	Layer two. Provides error-free transfer of data frames from one computer to another over the physical layer. In the context of the OSI reference model, a <i>frame</i> 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 layers above the data-link layer can assume virtually error-free transmission over the network.
Physical	Layer one. Establishes the physical interface and mechanisms for placing a raw stream of data bits onto the wire.

Note Protocols operating at different layers of the OSI model use different names for the units of data 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



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

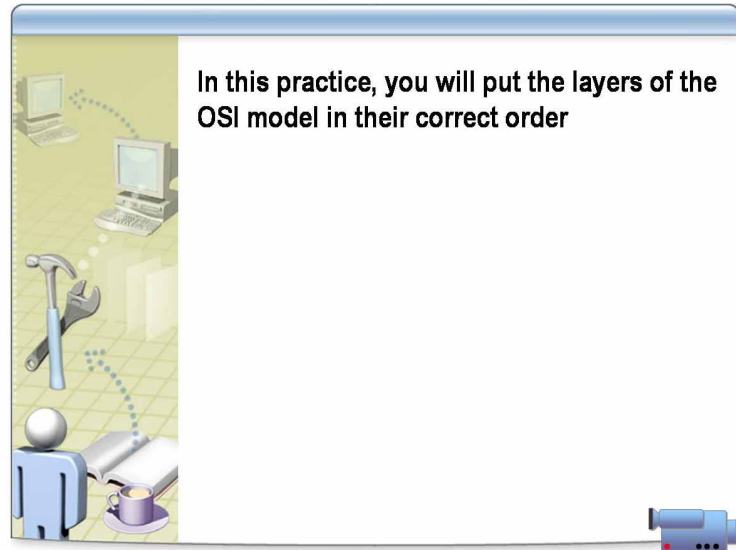
File location

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.

Practice: Putting the Layers of the OSI Model in Order



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

Introduction

In this practice, you will put the layers of the OSI model in their correct order.

File location

To perform the interactive multimedia practice, *Putting the Layers of the OSI Model in Order*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the practice.

Lesson: Overview of the TCP/IP Protocol Suite

- Why Do I Need to Know About TCP/IP?
- What Is the Architecture of the TCP/IP Protocol Suite?
- How Does the TCP/IP Model Relate to the OSI Model?
- How an IP Packet Moves Through the Suite of TCP/IP Protocols

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

Introduction

The protocols in the TCP/IP 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.

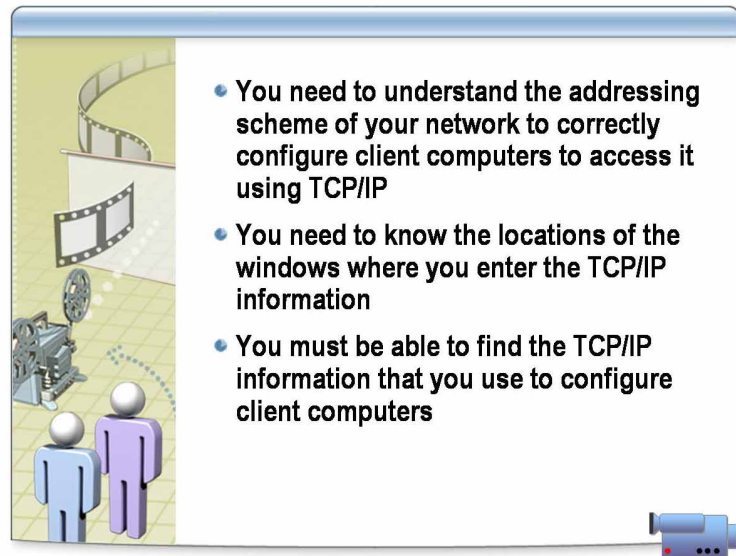
Note For more information about the TCP/IP protocol suite, see Request for Comments (RFC) 1180 under **Additional Reading** on the Student Materials compact disc.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the architecture of the TCP/IP protocol suite.
- Associate the protocols of the TCP/IP suite with those of the OSI model.
- Describe the function of the protocols at each layer of the TCP/IP model.
- Describe how a packet moves through the TCP/IP layers and what happens at each layer.

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



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

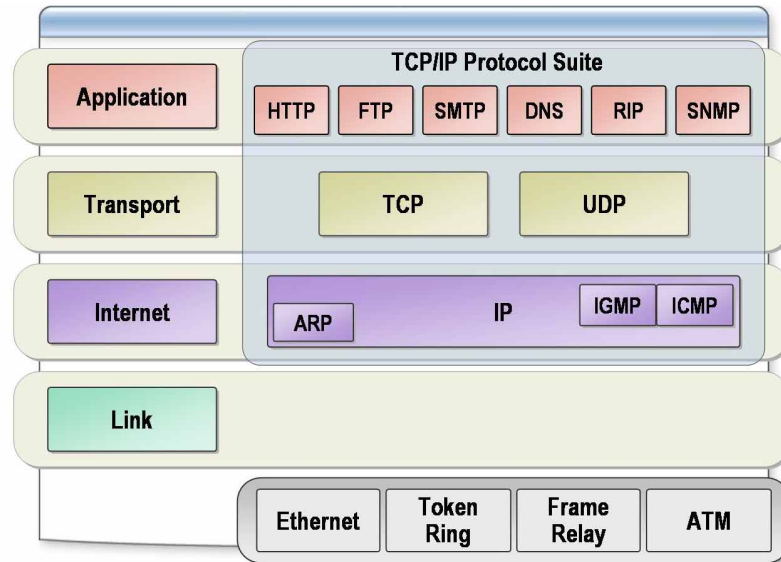
File location

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 Windows operating system.

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



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

Introduction

TCP/IP is an industry standard suite of protocols that provide communication in a heterogeneous environment. The tasks 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 as follows:

- The application layer
- The transport layer
- The Internet layer
- The link layer

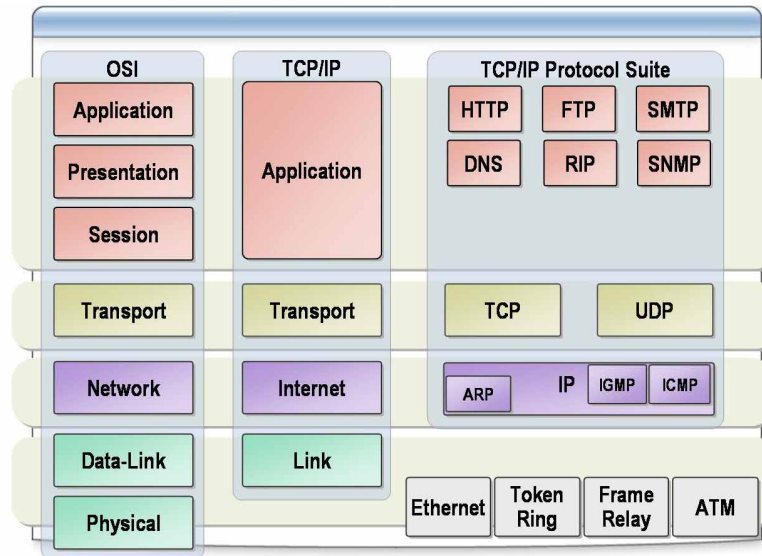
Benefits of TCP/IP

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 link layers, see RFC 1122 under **Additional Reading** on the Student Materials compact disc.

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



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

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. Two services at this layer that provide access to network resources are: Windows Sockets and Network Basic Input/Output Systems (NetBIOS). Both Windows Sockets and NetBIOS provide standard application interfaces for programs to access network services.

Application layer protocols

Some of the applications that operate at this layer connect or communicate with other network hosts 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 Transport Protocol. Carries e-mail messages between servers and from clients to servers.
DNS	Domain Naming System. Resolves Internet host names to IP addresses for network communications.
RIP	Routing Information Protocol. Enables routers to receive information about other routers on a network.
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
UDP	User Datagram Protocol. Provides connectionless communications and does not guarantee that packets will be delivered. Reliable delivery is the responsibility of the application. Applications use UDP for faster communication with less overhead than using TCP. SNMP uses UDP to send and receive messages on the network. Applications typically transfer small amounts of data at one time using UDP.
TCP	Transmission Control Protocol. Provides connection-oriented reliable communications for applications that typically transfer large amounts of data at one time, or that require an acknowledgment for data received.

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 packets, address them, and route them to their destinations.

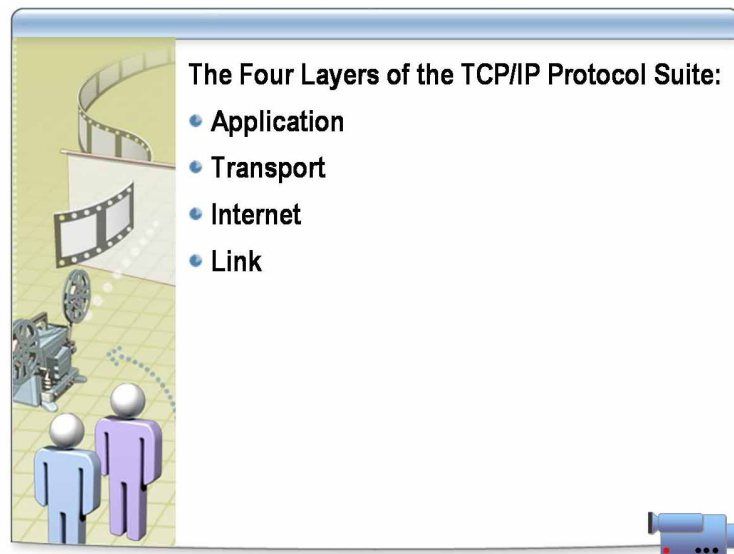
There are four protocols at the internet layer as described in the following table.

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.

Link layer

The link layer (sometimes referred to as the network 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. The layer is responsible for placing data on the physical network and for receiving data from the physical network.

Multimedia: How an IP Packet Moves Through the Suite of TCP/IP Protocols



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

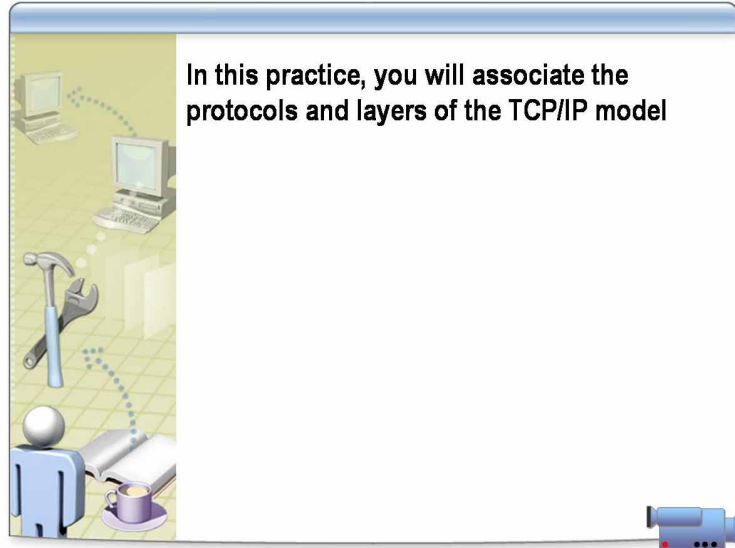
File location

To view the multimedia presentation, *How an IP Packet Moves Through the Suite of TCP/IP Protocols*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objective

After completing the 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.

Practice: Associating the Protocols and Layers of the TCP/IP Model



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

Introduction

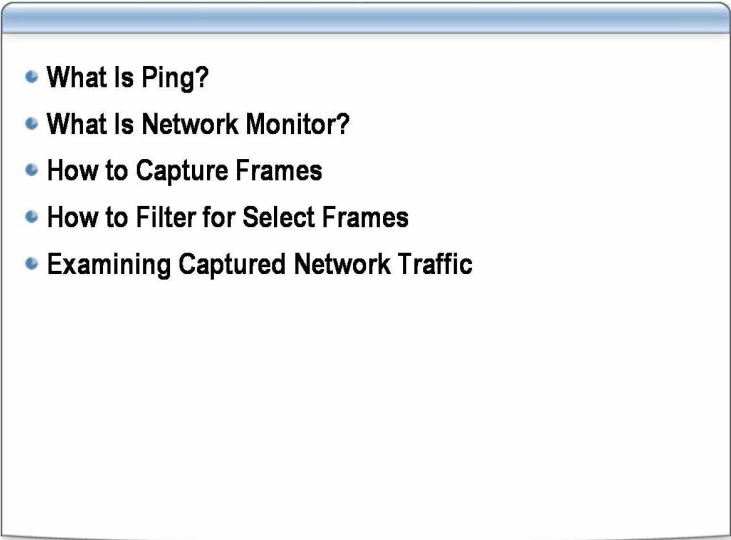
In this practice, you will associate the protocols and layers of the TCP/IP model.

Practice

► Associate the TCP/IP protocols with the OSI model

- To perform the multimedia practice, *Associating the Protocols and Layers of the TCP/IP Model*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the practice.

Lesson: Viewing Frames Using Network Monitor

- 
- What Is Ping?
 - What Is Network Monitor?
 - How to Capture Frames
 - How to Filter for Select Frames
 - Examining Captured Network Traffic

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

Introduction

Microsoft Network Monitor is a protocol analyzer that you can use to understand 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.

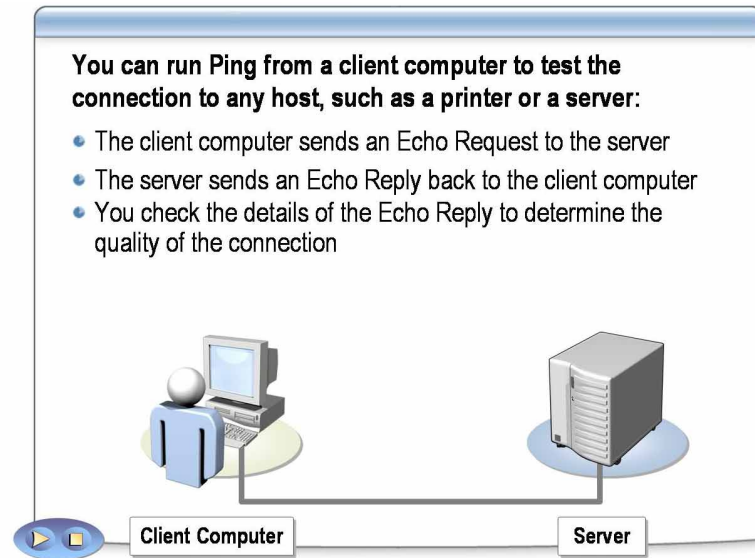
In this lesson, you will use the Ping utility (Ping) to generate traffic for analysis.

Lesson objectives

After completing this lesson, you will be able to:

- Use Ping to test network connectivity.
- Install Network Monitor.
- Capture network traffic.
- Set a filter to highlight specific captured frames.
- Describe the information that is captured by Network Monitor.

What Is Ping?



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

Introduction

TCP/IP implementations include a basic network utility called 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. In the preceding illustration:

1. The client computer is running the **ping** command specifying the server as the target computer.
2. Ping generates a series of Echo Request messages using ICMP and transmits the Echo Request 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 an 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 LONDON (192.168.2.10) with 32 bytes of data: Reply
from 192.168.2.10: bytes=32 time<10ms TTL=128
Reply from 192.168.2.10: bytes=32 time<10ms TTL=128
Reply from 192.168.2.10: bytes=32 time<10ms TTL=128
Reply from 192.168.2.10: bytes=32 time<10ms TTL=128 Ping
statistics for 192.168.2.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

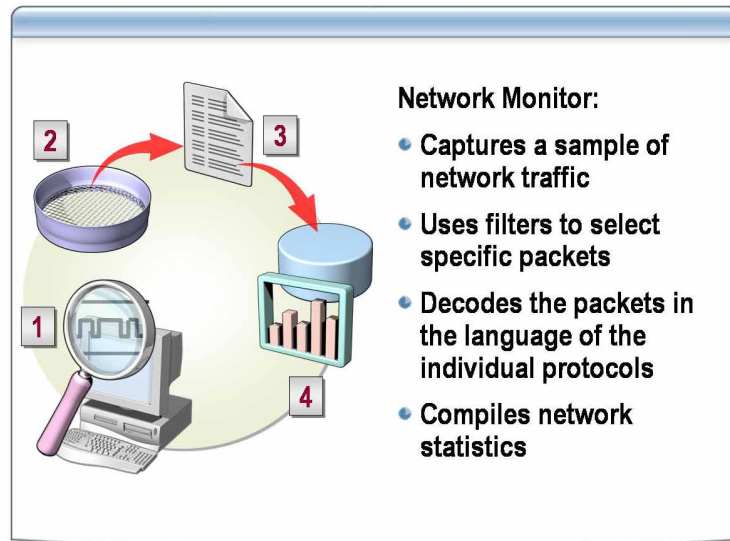
This display shows the echo replies from the target computer. Information displayed includes the IP address of the target computer, the number of bytes of data included with each request, the elapsed time between the transmission of each request and the receipt of each reply, and the value of the Time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

Note Because of security threats 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 echo requests.

What Is Network Monitor?



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

Introduction

Network Monitor is a utility included in Windows Server 2003, in Windows 2000 Server products, and in Microsoft Systems Management Server (SMS).

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.
- Identify unauthorized users on a network.

How it 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.

Versions of Network Monitor

There are two versions of Network Monitor: one that supports promiscuous mode and the other that supports nonpromiscuous mode:

- In promiscuous mode, the network adapter reads and processes all of the packets transmitted over the physical medium to which it is connected, and not just the packets addressed to it.

Caution Installing the promiscuous version of Network Monitor may be against your organization's security policy. Obtain appropriate permission before you install the promiscuous version of Network Monitor.

- In nonpromiscuous mode, the network adapter captures only traffic addressed to or transmitted by the computer on which Network Monitor is running.

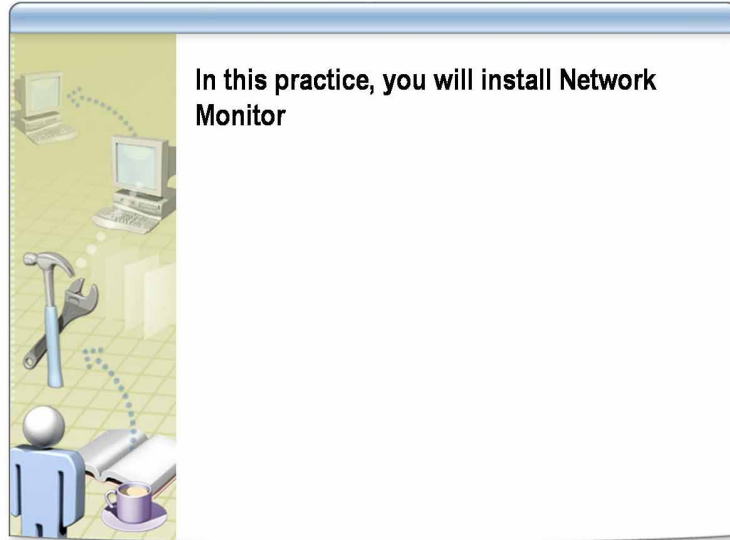
To run Network Monitor in promiscuous mode, you must have a network adapter capable of switching to that mode. Most, but not all, adapters can run in promiscuous mode.

SMS includes the version of Network Monitor that supports promiscuous mode. To increase security, the version that is included in Windows Server 2003, Windows 2000 Server, and Microsoft Windows NT® Server does not support promiscuous mode.

How to install Network Monitor

You install Network Monitor from the Windows Component Wizard. From **Subcomponents of Management and Monitoring Tools**, select the **Network Monitor Tools** check box, click **OK**, and then click **Next** to continue the installation.

Practice: Installing Network Monitor



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

Introduction

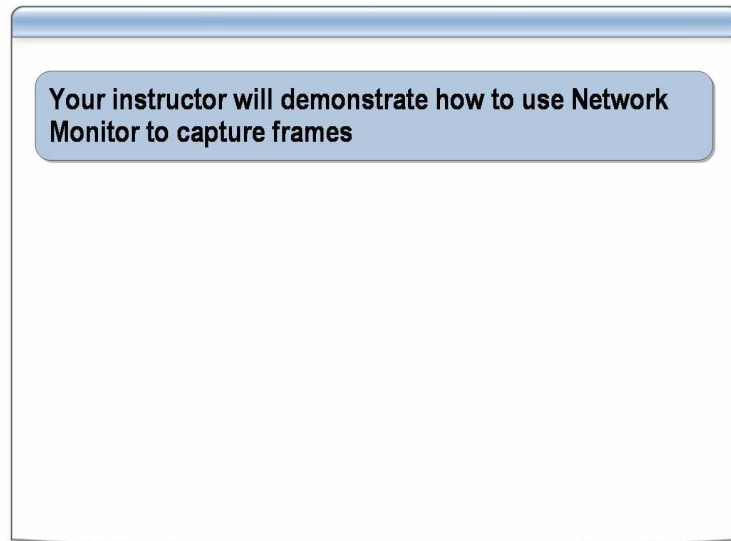
In this practice, you will install the promiscuous version of Network Monitor and create a Run as shortcut to run Network Monitor as Administrator while logged on as *ComputerUser*.

Practice

► Install Network Monitor

1. Log on to your computer with your *ComputerUser* account (where *Computer* is the name of your computer) and a password of **P@ssw0rd**.
2. In Control Panel, press SHIFT and right-click **Add or Remove Programs**.
3. Click **Run as**, and then click **The following user**.
4. In the **User name** box, verify that *Computer*Administrator appears.
5. In the **Password** box, type **P@ssw0rd** and click **OK**.
6. Click **Add/Remove Windows Components**.
7. In the Windows Components Wizard, click **Management and Monitoring Tools**, and then click **Details**.
8. In **Subcomponents of Management and Monitoring Tools**, select the **Network Monitor Tools** check box, and then click **OK**.
9. Click **Next**.
10. If you are prompted for additional files, click **OK**. In the **Copy files from** box, type **\\london\setup\i386** and then click **OK**.
11. Click **Finish**, and then close **Add or Remove Programs**.

How to Capture Frames



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

Introduction

Network Monitor enables you to capture frames of network traffic for analysis.

Procedure

► To capture frames by using Network Monitor

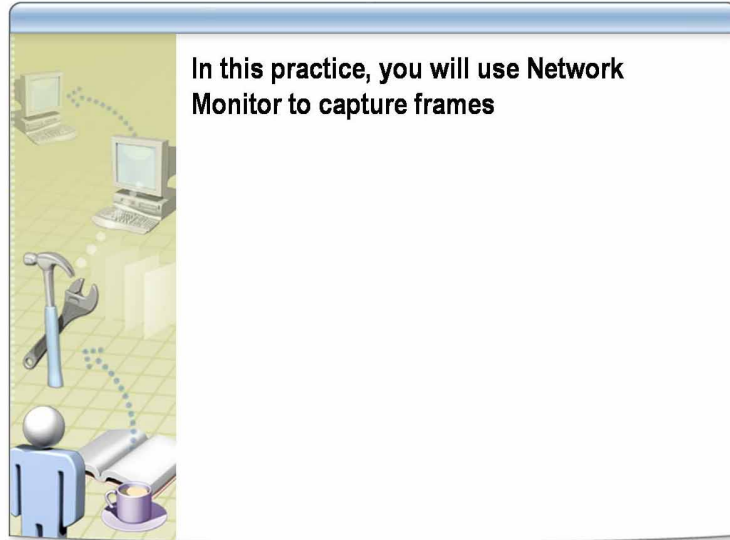
1. Open Network Monitor.
2. Select the network interface that you want to use (if it has not already been selected).
3. Start the capture process by clicking **Start Capture** on the toolbar.
4. To stop the capture, on the toolbar, click **Stop and View Capture**. Do not close the capture window.

Network Monitor can also be operated from the command line. For example, if you have already created a filter named http.cf, use the following command to start Network Monitor and use that filter:

```
start netmon /capturefilter d:\captures\http.cf
```

Note For more information about how to use Network Monitor from the command line, see Network Monitor online Help, and “Troubleshooting Performance” in the System Performance Troubleshooting Guide of the *Microsoft Windows Server 2003 Resource Kit*.

Practice: Capturing Frames



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

Introduction

In this practice, you will use Run as to open a command prompt and Network Monitor and then use Network Monitor to capture and display frames.

Scenario

You are the systems administrator for an organizational unit on a network and are isolating connectivity issues between two hosts. A protocol expert has requested that you capture ICMP traffic between the two hosts for further analysis.

Practice

► Start Network Monitor

1. On the **Start** menu, click **Control Panel** and then double-click **Administrative Tools**.
2. Press SHIFT and right-click **Network Monitor**.
3. Click **Run as**, and then click **The following user**.
4. In the **User name** box, verify that *Computer\Administrator* appears.
5. In the **Password** box, type **P@ssw0rd** and click **OK**.
6. If you are prompted to select a network, click **OK**.
7. In the **Select a Network** dialog box, expand **Local Computer**, click **Local Area Connection**, and then click **OK**.
8. Maximize the Microsoft Network Monitor window and the Capture window.

► Capture network data


- On the **Capture** menu, click **Start**.

This starts the data capture process. Network Monitor allocates buffer space for network data and begins capturing frames.

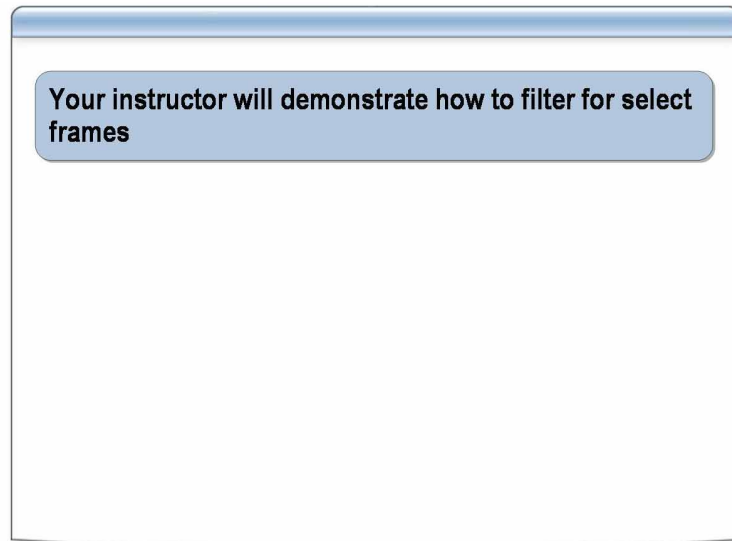
► **Generate and view network traffic**

1. On the **Start** menu, point to **All Programs**, point to **Accessories**, and right-click **Command Prompt**.
2. Click **Run as**, and then click **The following user**.
3. In the **User name** box, verify that *Computer\Administrator* appears.
4. In the **Password** box, type **P@ssw0rd** and click **OK**.
5. At the command prompt, type **arp -d *** and press ENTER.
6. At the command prompt, type **ping 192.168.x.200** (where *x* is your classroom number), and then press ENTER.

► **Stop the network data capture**

1. Switch back to Network Monitor.
2. On the **Capture** menu, click **Stop and View** .
Network Monitor stops capturing frames and displays them.
3. Leave the Capture window open.

How to Filter for Select Frames



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

Introduction

On a busy network, a packet capture of only a few seconds can consist of thousands of frames, generated by dozens of different systems. You can define capture filters so that only specific frames are saved for analysis. For example, if you want to learn how much network traffic is generated by ARP transactions, you can create a filter that captures only ARP traffic for a specific period of time, and then calculate the number of megabits per hour devoted to ARP from the size of your captured sample.

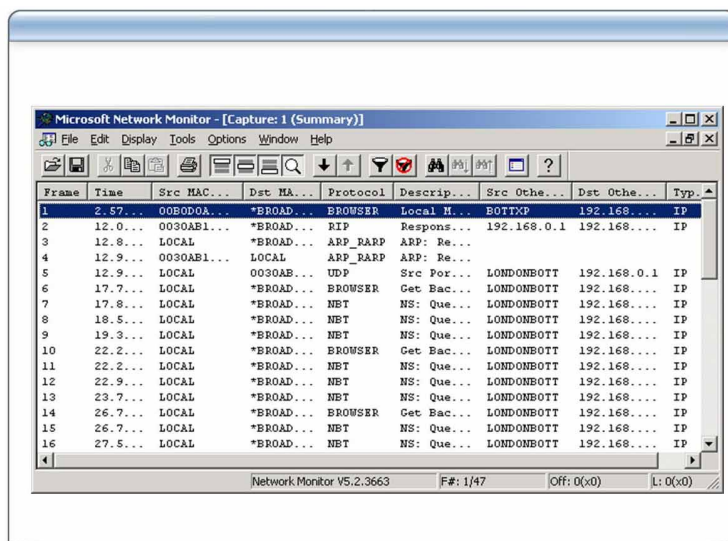
Procedure

The following steps outline the procedure to filter only ARP packets when capturing network traffic.

1. Open Network Monitor.
2. On the **Capture** menu, click **Filter**.
3. If using the nonpromiscuous version of Network Monitor, click **OK** to close the **Microsoft Network Monitor** dialog box that describes security. Otherwise, proceed to Step 4.
4. Click **SAP/ETYPE=Any SAP** or **Any ETYPE**.
5. Click **Edit**, and then click **Disable All**.
6. In the **Disabled Protocols** list, click **ARP**, and then click **Enable**.
7. Click **OK** to close the **Capture Filter SAPs and ETYPES** dialog box.
8. Click **OK** to close the **Capture Filter** dialog box.
9. Start, stop, and view the capture.

The Network Monitor Capture Summary window displays the summary record of all frames.
10. Leave the Capture window open.

Examining Captured Network Traffic



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

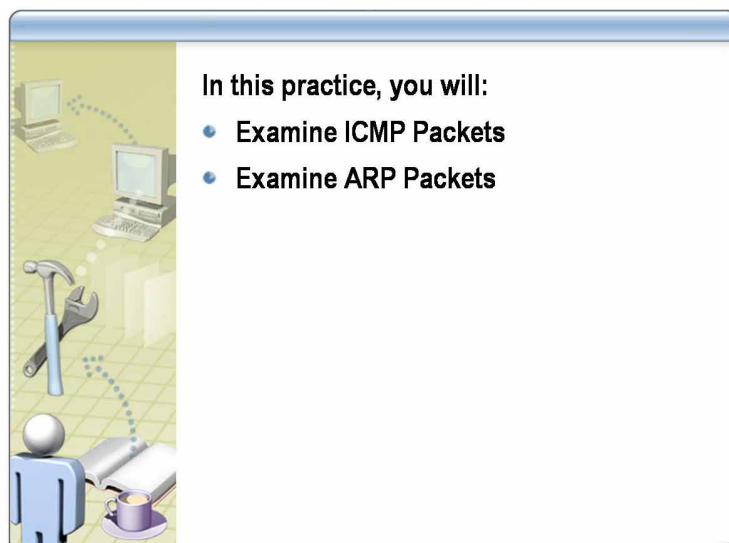
Introduction

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) that 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 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.
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: Examining Packets



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

Introduction

In this practice, you will change the color of all frames that use ICMP. This is useful when viewing frames for a particular protocol. You will also use Network Monitor to capture and examine ARP packets.

Practice

► Examine ICMP packets

1. On the **Display** menu, click **Colors**. The **Protocol Colors** dialog box appears.
2. Under **Name**, click **ICMP**.
3. Under **Colors**, set foreground to red, and then click **OK**.

The Microsoft Network Monitor Capture Summary window appears, displaying ICMP frames in red.

► Examine ARP packets

1. On the **Window** menu, verify that **Summary**, **Detail**, and **Hex** are selected.
2. On the **Window** menu, verify that **Zoom Pane** is deselected.

Three separate panes are displayed. The top pane displays the frame summary, the middle pane displays the selected frame details, and the bottom pane displays the selected frame details in hexadecimal notation. As you click in each pane, the window title bar updates with the name of the pane.

3. In the Summary pane, in the Description column, click an ICMP frame that has an entry beginning with **Echo: From** in the description column.

This frame shows an ICMP echo request from your computer to the instructor computer.

4. In the Detail pane, click **ICMP** with a plus sign (+) preceding it. The plus sign indicates that the information can be expanded by clicking it.

5. Expand **ICMP**.

The ICMP properties expand to show more detail. The contents of the ICMP packet are highlighted and displayed in hexadecimal notation in the bottom window.

6. In the Detail pane, click **ICMP: Packet Type = Echo**.

What hexadecimal number corresponds with ICMP: Packet Type = Echo?

Answer: 08

7. In the Detail pane, click **Checksum**.

Record the Checksum number in the table below.

8. In the Detail pane, click **Identifier**.

Record the Identifier number in the table below.

9. In the Detail pane, click **Sequence Number**.

Record the Sequence Number in the table below.

10. In the Detail pane, click **Data**. The data received in the echo message must be returned in the echo reply message.

11. Repeat steps 1 through 9 for the Echo Reply packet that follows the Echo: From packet that is currently displayed.

12. Close Microsoft Network Monitor and do not save the capture.

Field	Echo	Echo Reply
Packet Type	Echo	Echo Reply
Checksum	A number <i>n</i>	A number different from <i>n</i>
Identifier	Numbers should be the same for Echo and Echo Reply	
Sequence Number	Numbers should be the same for Echo and Echo Reply	

The Packet Type changed from Echo to Echo Reply. The Checksum will change (numbers will vary). The Identifier is the same for all ICMP packets and Sequence Numbers remain the same for all echo packet pairs.

