# Lesson 3: Network Protocols

## At a Glance

Since switches utilize both Layer 2 and Layer 3 protocols, it is necessary to understand the concept of network addressing and the protocols used at both the data link and network layer of the OSI model. Several of these protocols were covered in the *NetKnowledge Internetworking Fundamentals* and *Routing* courses. In addition to reviewing previously covered addressing protocols, this lesson introduces the concept of dynamically assigning TCP/IP addresses. Dynamic Host Configuration Protocol, DHCP, is the protocol that is used to dynamically assign addresses from a pool of available addresses.

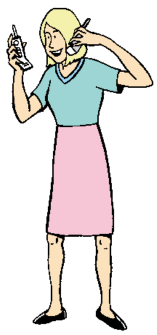
## What You Will Learn

After completing this lesson, you will be able to:

- Explain how switches use Layer 2 protocols to segment a network and obtain hardware addresses
- Describe TCP/IP protocols and their relationship to switching
- Explain the function of BootP, TFTP, and ARP
- Describe DHCP and explain its importance in networking
- Differentiate between RIP and OSPF

## Student Notes:

## Tech Talk



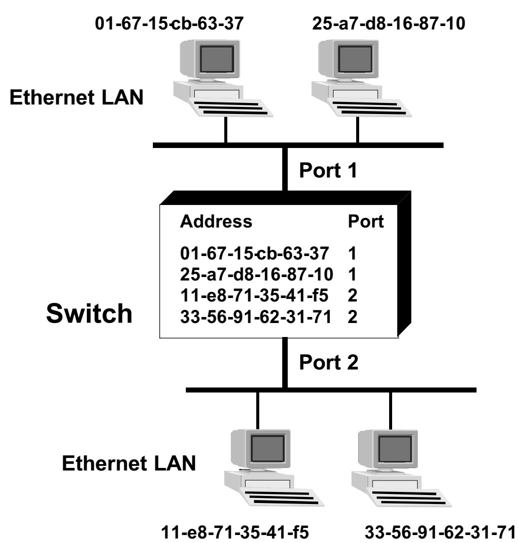
- **Datagram**—Packets of data at the network layer.
- **Frame**—Basic unit of data transfer at OSI Layer 2.
- **Frame Relay**—A WAN protocol, packet switching, connectionless service.
- **Packet**—A basic unit of data transfer at OSI Layer 3.
- **Packet Switching**—A switched connection for WANs in which data from many different LANs may share a single circuit. Data is encapsulated in packets (sometimes called frames or cells) for transmission.
- **Spanning Tree Algorithm**—Algorithm used to ensure a loop-free topology by enabling a single path through the network.
- **Transmission Control Protocol/Internet Protocol (TCP/IP)**—The entire suite of protocols used internationally to access the Internet.
- **User Datagram Protocol (UDP)**—A connectionless transport method used to transmit messages between the Network Management System (NMS) and the agent. UDP is a standard member of the TCP/IP protocol suite.

## Switching and Networking Protocols

Switching hubs are Layer 2 devices and function at the data link layer of the OSI model. They are used to separate networks into logical segments. Each segment then becomes its own collision domain, yet it remains in the same broadcast domain. This reduces network congestion because Layer 2 switches forward data to other segments only if it is destined for a device on that other segment. Only transmissions addressed to different segments can pass through the switch. Transmissions addressed to the same segment stay within that segment. This is accomplished by building a table of the MAC hardware addresses and their corresponding ports for all devices connected to the network.

The job of the Layer 2 switch is to check the MAC address against the port and send the data to the correct port. Layer 2 switches do not broadcast the message to the other ports. This saves valuable bandwidth and allows network managers to configure networking segments in such a way that each device can have a dedicated connection, thus eliminating collisions. Layer 2 protocols include Ethernet, Token Ring, and other 802.x IEEE standards. Data link layer protocols don't know and don't care what protocols are running on the above OSI layers. They can therefore connect different network types, for example, Ethernet and Token Ring.

### Associating MAC Addresses with Ports



In addition to performing the functions of a Layer 2 switch, Layer 3 switches can accomplish routing functions. Switching routers use Layer 3 protocols such as RIP OSPF, and NLSP to route data among different networks. Subsequent lessons discuss the similarities and differences between layer 2 and layer 3 switches and switching technology. The protocols that follow are important to understand when discussing data transmission via switches.

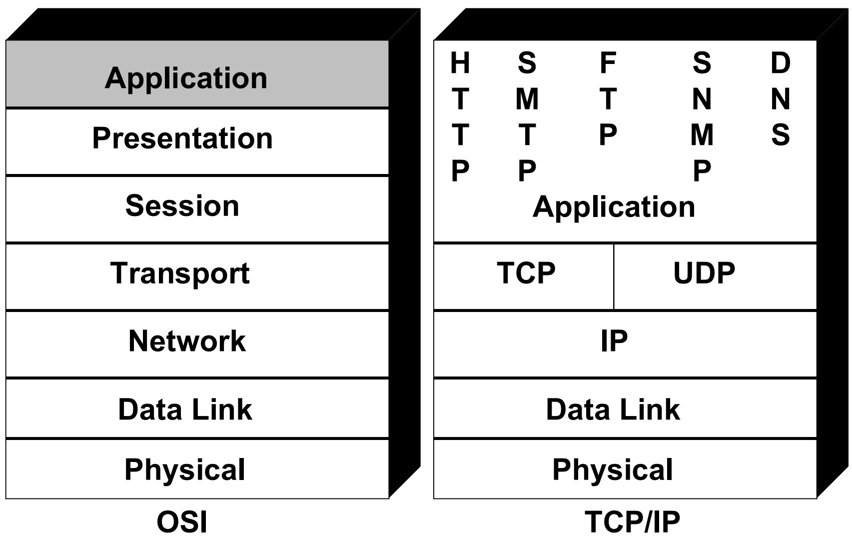
## Check Your Understanding

- Explain how Layer 2 switches help eliminate broadcast traffic.
- Why is this important?

## Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP was developed in the mid-1970s to allow different kinds of computers to communicate. Although there were other protocols available at the time, TCP/IP was freely available and popular at universities. With the rise of the Internet, TCP/IP has become increasingly popular and is the protocol used for communication over the Internet.

### TCP/IP vs. OSI Model




TCP/IP follows the OSI model for the lower 4 layers, but combines the upper 3 layers, session, presentation, and application into a single layer. TCP/IP operates independently of the physical and data link layers, using a frame as its data unit. At the network layer, Layer 3, the Internet Protocol delivers data across networks. At the transport layer, Layer 4, TCP (a connection-oriented protocol) pairs with a connectionless protocol, UDP (User Datagram Protocol) to provide process-to-process delivery of data across networks. In its uppermost application layer, TCP/IP handles the functions that are most familiar: email, web browsing file transfers, etc.

## TCP

Transmission Control Protocol (TCP) is a transport layer protocol that provides end-to-end reliable delivery, port addressing, and flow control. TCP provides error checking and reporting using a checksum. If a packet arrives damaged, the failure is reported and the sender can retransmit the packet.

A feature of transport layer protocols is segmentation—the division of a single message into multiple pieces. Sequence control ensures that all packets of the original message are received in the proper order. To do this, TCP includes a sequence number in the header of each packet that is to be transmitted across the network. These numbers are used to put the packets in the correct order when the destination device receives them.

Along with sequence control is loss and duplication control. TCP ensures that not only are packets received error-free and in the correct order, but no packets have been lost in transmission. TCP also makes sure that no packets are duplicated.

To ensure that the receiving device is not overwhelmed with a flood of data, TCP provides flow control. If data is coming in too fast, TCP informs the receiver to reduce the data rate until it can catch up.

## Check Your Understanding

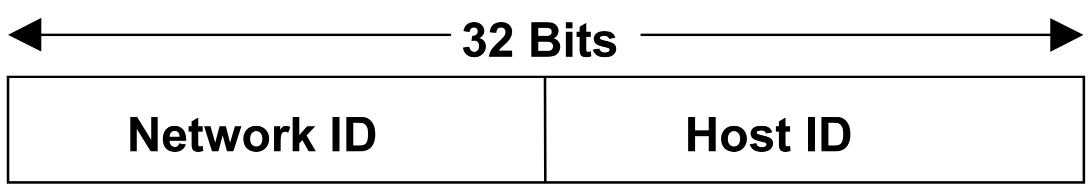
- What is the main function of the TCP protocol?
- Why is flow control important?

## IP

The primary function of Internet Protocol (IP) is to accept data from the higher layer protocols (TCP, and UDP) on a source host, create a datagram, and route the datagram through a network to a destination. In order to transmit this data over the Internet, a device must have an IP address and learn the IP address of the destination device. IP, a connectionless protocol, is the Layer 3 (network) component of the TCP/IP protocol suite that provides network layer functionality to move data from network to network across an internetwork. IP moves data over data link and physical layer protocols. This allows an internetwork to be a combination any transmission medium; media access method, physical addressing, and topology. IPv4 is current standard. IPv6, which uses 128-bit IP addresses, is a newer version of the IP standard that was developed to meet the demand for more addresses than IPv4 is able to offer.

When a network connects to the Internet, each device must have a unique IP address, which is assigned by an Internet authority. Just as the postal service uses unique house addresses to route mail from a source address (sender) to a destination address (receiver), IPv4 uses a device's unique 32-bit address for routing data from a source device to a destination device. The IPv4 address consists of four groups of numbers (each group between 0 and 255) separated by periods, sometimes called dotted decimal notation. Even networks that are not connected to the Internet use IP addressing because it is a standard way of addressing devices. IP addresses, you may recall, are unique for each network. The first part of the IP address indicates on which network a device is located. The second part of the IP address indicates a particular device (or host) on that network.

**IPv4 32-Bit Address**

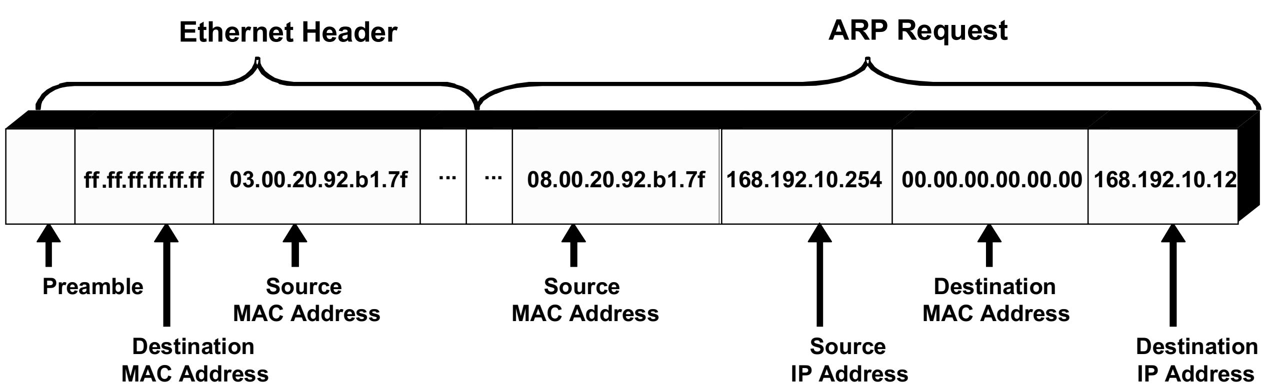


A network administrator must assign each device on his or her network one of the IP addresses they have been allocated. This is done either statically or dynamically. Static IP addresses must be configured individually at each computer device. When the device is moved to another part of the network, a new IP address must be configured. Dynamic assignment of IP addresses is done using Dynamic Host Configuration Protocol (DHCP), a network IP management protocol. This protocol allows a network administrator to centrally manage the automatic assignment of IP addresses.

### ARP

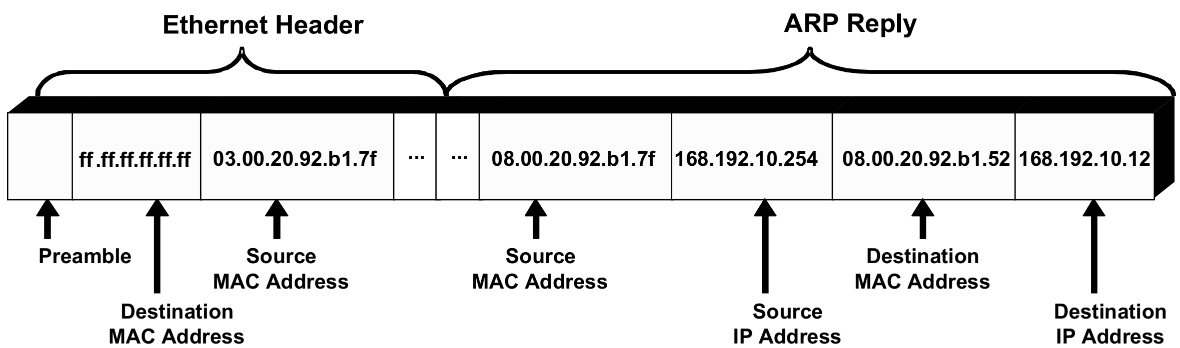
Address Resolution Protocol (ARP) is an interface protocol between Layer 3 and Layer 2 protocols. If a source device does not know the MAC address of a destination device, it sends out an ARP request, which is a broadcast transmission. Switches separate collision domains but do not separate broadcast domains; therefore, all segments on the network receive the ARP request.

### ARP Request Frame



An ARP request contains both the IP and MAC addresses of the source destination. All devices receiving the broadcast add this data to their ARP tables. The device with the destination IP address makes an entry and sends an ARP reply to the source device.

## ARP Reply Frame




This reply contains both its IP and MAC addresses, which the source device then adds to its ARP table. It can now send data to the destination device because it can map the MAC address with the IP address.

RARP, or Reverse Address Resolution Protocol, functions much the same way except it associates a known MAC address with an unknown IP address.

### BootP

Bootstrap (BootP) is a protocol that uses data link layer protocols, User Datagram Protocol (UDP), and Trivial File Transfer Protocol (TFTP) to translate MAC source and destination physical addresses into IP logical addresses, and to receive boot files.

BootP uses a database that translates a MAC hardware address into an appropriate IP address. The system administrator must enter all of the database information. This process is time consuming and tedious. Configuration errors are not uncommon and can cause serious networking problems. This was one of the major motivators for the dynamic host configuration protocol (DHCP) protocol, BootP's successor.

The exchange of MAC to IP addresses is accomplished using a packet exchange. The BootP packet contains information about the client device, such as the type of network, the number of seconds since the client started to boot, IP address if known, etc. It uses this information to obtain the appropriate MAC and IP addresses for the destination device.

## BootP Packet

| Operation (1)* | Hardware type (1) | Harware address length (1) | Hops (1) |
|---|---|---|---|
| Transaction ID (4) | | | |
| Seconds (2) | | Flags (2) | |
| Client IP address (4) | | | |
| Your IP address (4) | | | |
| Server IP address (4) | | | |
| Gateway IP address (16) | | | |
| Client hardware address (16) | | | |
| Server name (64) | | | |
| File name (128) | | | |
| Vendor-specific area (64) | | | |
| * The number in parentheses indicates the number of octets in each field. | | | |

BootP uses the client-server model to enable devices to boot from the network. To broadcast a request for an IP address, a client sends a BOOTREQUEST. When the request is sent, a timer is set. If the time expires before a reply is received, the BOOTREQUEST is resent.

**TFTP**

Trivial File Transfer Protocol (TFTP) is a simple, easy-to-implement protocol within the User Datagram Protocol (UDP) that can be used for remote network operating system installation in conjunction with BootP.

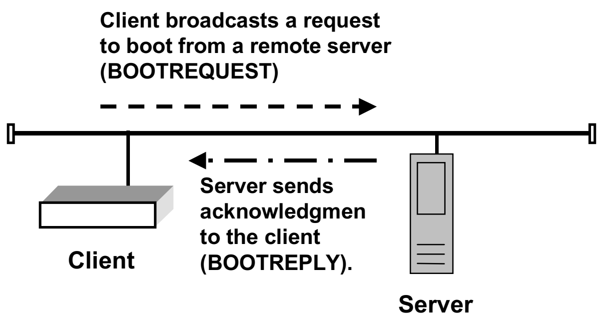
TFTP is a program that is built into the programmable read-only memory (PROM) of a device and executes the commands necessary to get BootP data back and forth between the boot server and the client device.

There are five types of TFTP packets:

- Read Request (RRQ)
- Write Request (WRQ)
- Data (DATA)
- Acknowledgement (ACK)
- Error (ERROR)

BootP and TFTP each use a two-step process. The first process is a request to the BootP server for startup information. The reply contains the information needed to initiate a TFTP request. This reply specifies the name of the TFTP file that contains the initial memory image, or software image. The second step requests the initial memory image required to complete the startup operation.

## Two-Step BootP/TFTP Startup Process



### DHCP

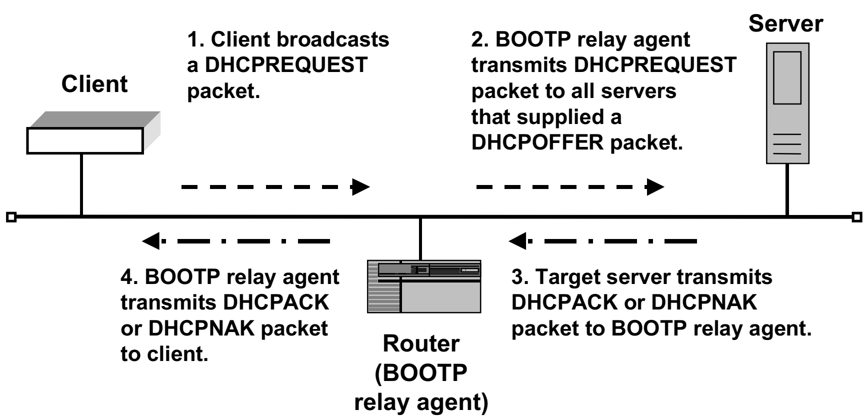
DHCP is an extension of BootP that allows network managers to assign IP addresses dynamically by way of a centrally managed DHCP server. This eliminates the need to manually maintain a table of MAC and IP addresses for every device on a network.

DHCP has two primary purposes. The first is the same as BootP, to notify a host of its IP address when connecting to a network. However, DHCP has the ability to assign, or lease, IP addresses for a fixed period of time. The network manager determines this time frame, and it can range from as little as one minute to as long as 99 years. Secondly, DHCP also acquires other configuration parameters for clients.

Leasing IP numbers for short periods of time via DHCP provides an essential service for today's networks. Rather than have an IP address for each client on a network, clients can lease numbers for short periods of time. People travel, they are out sick, and they work from their homes. They do not need to have permanent IP addresses.

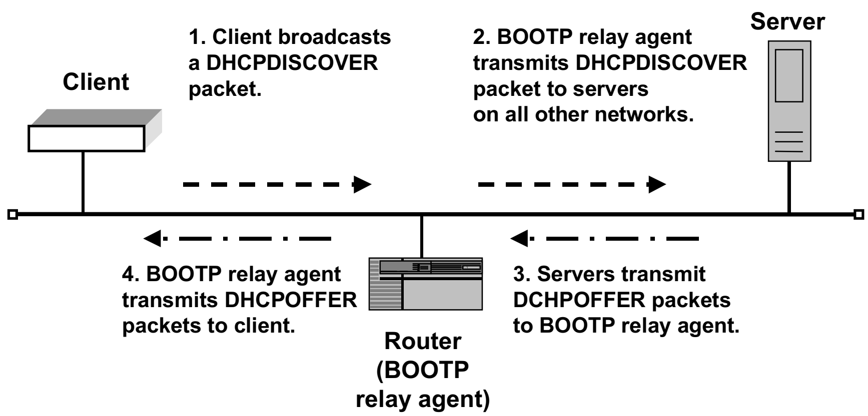
---

## DHCPREQUEST



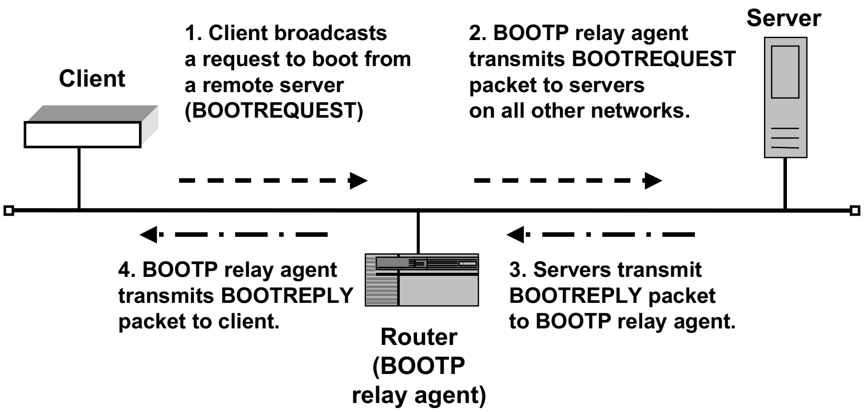
The DHCP packet format is based on a BootP packet and uses a BootP relay agent to forward DHCP packets as follows:

**DHCPDISCOVER**




- A client broadcasts a DHCPDISCOVER packet.
- A BootP relay agent receives the packet, accepts the packet, and forwards it to DHCP servers on other networks.
- DHCP servers transmit a DHCPOFFER packet, which contains an available IP address, to the BootP relay agent.
- The BootP relay agent receives the DHCPOFFER packets and forwards them to the client.
- The client examines the configuration parameters of the packet and decides which DHCPOFFER to accept.

## BOOTREQUEST




- After selecting a DHCPOFFER, the client inserts the IP address of the target server into the packet and broadcasts the BOOTREQUEST packet.
- The router, or switch-router, forwards the packet to all the servers that sent DHCPOFFER packets. If the IP address in the DHCPOFFER does not match, the DHCP server reclaims the unused IP address.
- The target server recognizes its IP address in the server IP address field and responds with a DHCPACK, which is sent to the client through the BootP relay agent.
- The client examines the configuration parameters in the DHCPACK and records the duration of the lease period. If there is a problem, it sends a DHCPDECLINE and the process starts again.

## Check Your Understanding

- Describe the function of IP.
- Describe ARP.
- What is the main difference between BootP and DHCP?
- Why is this important?
- What are the two-steps of the BootP/TFTP startup process?

## Check Your Understanding (continued)

- Give a situation where a network manager would want to statically assign an IP address?
- Give a situation where a network manager would want to dynamically assign an IP address?
- What are the main purposes of DHCP?
- List the steps that BootP uses to discover DHCP servers and obtain IP addresses.

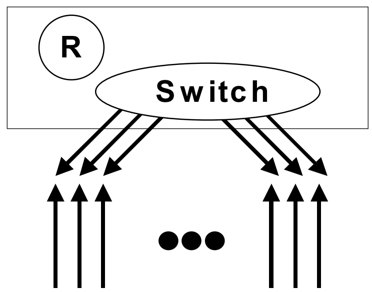
## Routing Protocols

In order to transmit data across networks, the data must be routed. Until very recently, switches were Layer 2 devices and not capable of routing across networks. Today, in addition to maintaining MAC addressing data, which assists with directing traffic, switches typically connect to and/or extend similar or dissimilar network segments, and allow for the creation of virtual local area networks (VLANs). They also allow managers to establish single and/or multiple host collision domains within LANs.

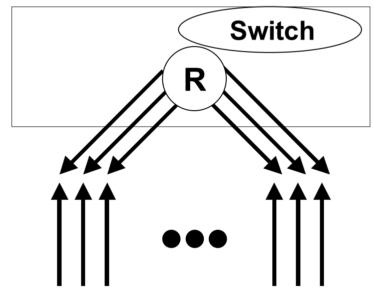
Today's switching routers can route across, not just within, networks. Switching routers, sometimes called Layer 3 switches, allow separate networks to maintain their logical identity. This means that when network A connects to network B through a switching router, the two networks remain separate LANs, each with its own distinct network IP address.

Layer 3 switches are able to route data faster than routers because some of the routing protocols previously handled by routing software are now built into the hardware of the switching routers. As a general rule of thumb, with regard to software and hardware, when the information is built into the hardware it is always faster than software.

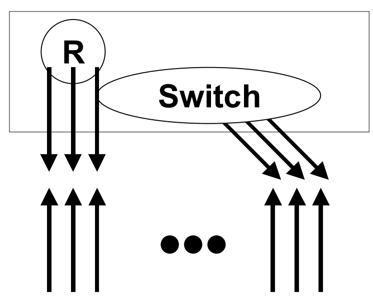
### Layer 3 Switches Allow Flexible Configurations




**Layer 2 Switch**




**A Router**



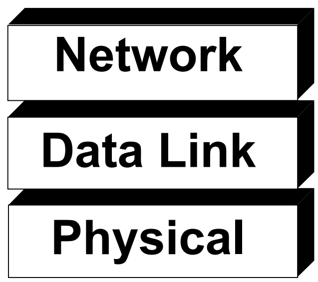

**Router or Switch**

Decisions about how data is routed across networks, whether through a router or switching router, are typically made using either distance-vector and/or link-state algorithms. For example, when driving home after a ballgame or concert, you make choices. Should you take the interstate highway, which is the shortest route and usually the fastest? Or, should you take a less traveled more circuitous route, which means traveling several additional miles? How do you make the decision if you want to get home as quickly as possible? If it's late at night, traffic is not a problem; the interstate highway is the fastest route. This decision is based on a distance-vector algorithm, or the shortest distance from point A to point B.

However, if you are heading home during the nightly rush hour the route that is five miles longer, more circuitous, and doesn't have the rush hour traffic, is probably the better choice for the fastest route home. In computer terms, this is similar to a link-state protocol solution. And, in this case would be the better choice for determining the fastest route.

Both routers and switching routers use Layer 3 routing protocols to move data traffic from one network to another network via the fastest route(s) available. Two commonly used routing protocols are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

**Both Routers and Switching Routers use Layer 3 Protocols**




**RIP**

The Routing Information Protocol (RIP) is one of the oldest routing protocols. RIP is a distance-vector protocol first described in theory in the late 1950's and included as part of network computer operating systems in the 1960's. After several years of proprietary RIP protocols, a standard protocol was agreed upon in 1988.

RIP packets are used to quickly calculate the distance between two points over a variety of routes. The best route, or shortest path, is reported back to the source device. A data base containing the information discovered is maintained in the routing tables of the routing device. RIP does not take into consideration such things as congestion, line speed, and cost.

Routing tables list, update, and share with other routing devices the incoming and next IP addresses, metrics (distances), and flags that indicate an entry changed recently. When a change is made to a routing table, it is shared with the routing devices that are directly connected to this router. These connected routing devices are often referred to as immediate neighbors. A list of routes presently known by a router is broadcast every 30 seconds. RIP allows a maximum of 15 hops because of the time it takes for all routers to stabilize their routing tables. If a device is 16 hops away, that means it is unreachable. Extended RIP allows up to 127 hops, although this is not recommended.

## RIP Routing Table

| Destination | Metric | Next Hop | Type | Protocol | Age | Index |
|---|---|---|---|---|---|---|
| 192.32.1.0 | 0 | 192.32.1.90 | Direct | Local | 12 | 1 |
| 192.32.2.0 | 0 | 192.32.1.81 | Direct | Local | 15 | 2 |
| 192.32.3.0 | 2 | 192.32.1.80 | Indirect | RIP | 27 | 2 |
| 192.32.4.0 | 2 | 192.32.1.91 | Indirect | RIP | 16 | 1 |

### OSPF

In the 1980's as networks grew larger, it became obvious that a faster, more efficient routing algorithm was needed. RIP works well for smaller networks, however it is not a scalable protocol. Networks can only expand up to 15 routers and by default, routing tables are updated every 30 seconds. The time it takes to recalculate distance vectors for each device addition or change bogs down larger networks. This led to the development of the Open Shortest Path First (OSPF) link-state protocol.

Unlike RIP, which examines the distance between two points on a network OSPF uses a link-state algorithm. With link-state protocols, a network administrator can set the Type of Service (TOS) values on an arbitrary basis, such as the speed of the data transmission or the fault tolerance of a link.

The way in which OSPF is able to improve network traffic starts by limiting itself to IP as the protocol. Without having to take the time to interpret other packets, routing tables can be constructed. For routing table data, OSPF breaks networks into sections and only looks at small sections and not the entire network enterprise. By breaking the network up into smaller pieces, called areas, OSPF can move packets more efficiently. Areas are not defined by geographical location (i.e., not just the hosts and routers physically closest to each other) but by traffic patterns.

### A Comparison of RIP and OSPF

| **Feature** | **RIP** | **OSPF** |
|---|---|---|
| **Algorithm Type** | Distance-Vector | Link-State |
| **Maximum Hops** | 15 | Limited only by size of routing tables that the device can hold |
| **Mask** | RIPv1 allows just one mask for the entire network | Can have variable length subnet masks |
| **Routing Metric** | Hop count | Calculated cost |
| **Complexity** | Relatively simple | Complex with many configurable parameters |
| **Convergence** | Slow | Fast |
| **Routing Update Frequency** | Broadcasts on a regular basis regardless of changes | Sends routing update only when something has changed |
| **Update Message Contents** | Networks in the autonomous system/hop count | Directly connected networks, mask, cost |

The concept of areas limits downtime, routing table edits, and other parameters to one area of a network. This fact enables networks employing OSPF protocols to scale easily.

## IPX

For many years, especially in the 1980's and well into the 1990's, Novell's NetWare operating system represented more than 80% of all installed networks in the United States. This was prior to the recent popularity and industry-wide acceptance of the Internet and its readily available TCP/IP protocols. Novell used their own proprietary IPX/SPX protocols for data transmission across networks.

Internetwork Packet Exchange (IPX) and Sequenced Packet Exchange (SPX) are analogous to TCP/IP protocols. IPX provides routing services similar to the ones provided by IP, and SPX is a connection-oriented protocol, similar to TCP. IPX runs on Layer 3 of the OSI model.

IPX packets can be anywhere from 30 bytes long to 65,535 bytes long, but usually are limited by network configuration to be about 1500 bytes. For many years, NetWare provided IPX packets using RIP as the routing protocol, but more recent versions of NetWare route IPX packets using Novell's version of the link-state routing algorithm, NetWare Link Services Protocol (NLSP).

The latest versions of NetWare now support the use of TCP/IP as well as their proprietary routing schemes.

## Check Your Understanding

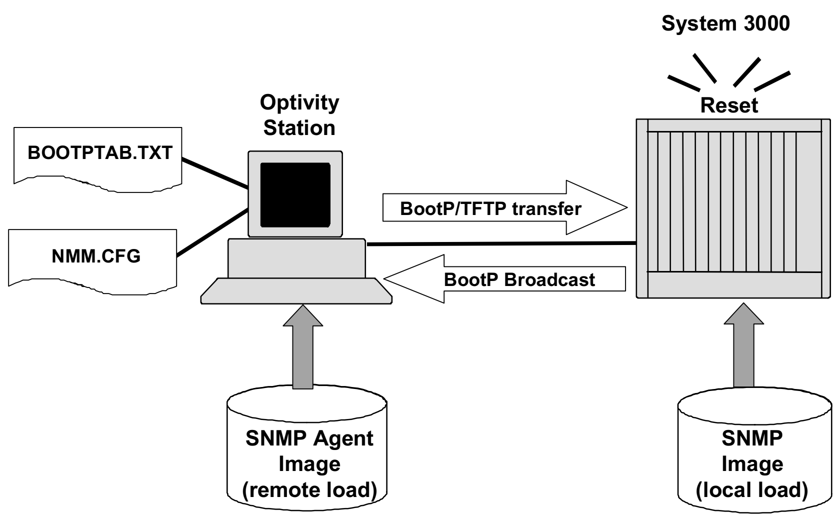
- What is the purpose of routing protocols?
- Which routing protocol is link-state?
- Which routing protocol is a distance vector algorithm?
- Compare and contract OSPF and RIP.
- What is IPX and what does it do?

## Management Protocols

### SNMP

Simple Network Management Protocol (SNMP) is a connectionless network management protocol that uses the UDP transport layer of TCP/IP. It uses an agent-manager model for communication between network devices.

### SNMP Station and Devices with SNMP Agents

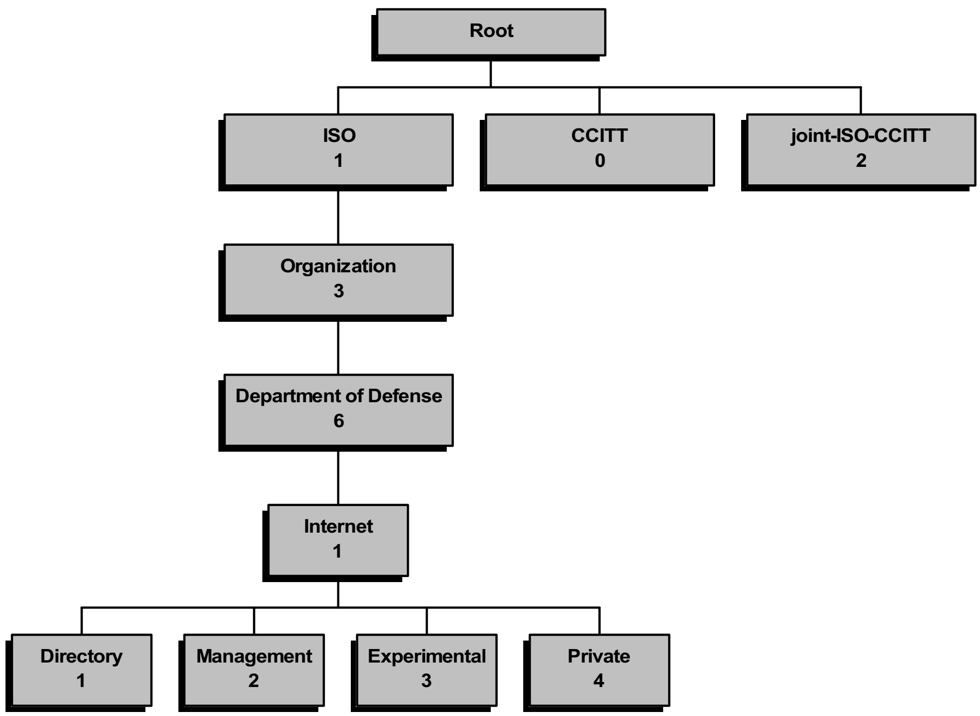



In SNMP, the collection of information is distributed among various devices, called agents, on the network. A centralized management station, running another piece of SNMP software, analyzes and interprets the data. Each agent stores data about its status and operations in a database and has the capability to alert a designated management station when problems occur.

**MIB**

The management information base (MIB) is a database that contains information about the managed object, its interfaces, the transmission medium to which it is attached, the protocols that it runs, and any vendor-specific information that a management system collects. The SNMP agent collects the information and stores it in the MIB. When the agent receives a request for information from the management station, the agent queries its MIB, from which it gets data to respond to the management station query.

## Management Information Base




Every MIB has a tree-like structure that consists of a root connected to a number of labeled object groups. Each group may branch to another sub-layer of objects. Within each object is the object instance or variable that is read or modified by SNMP.

The path from the root through the tree's branches to a specific object identifies the object. The ISO defines the root of the tree. Different vendors define the other branches of the tree for use with their products.

## Check Your Understanding

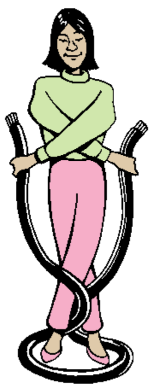
- What is SNMP?
- Why is this useful to a network manager?
- What are MIBs?

## Try It Out

**Materials Needed:**

- Internetworking Fundamentals Research Materials
- Internet Connection (optional)
- Presentation Evaluation Form

**Classroom Networking Presentation**



This lesson is a brief review of material covered in the *Internetworking Fundamentals* course. A thorough understanding of internetworking fundamentals is a prerequisite for success in this Switching and Network Management course.

When you embark on your career, whether it is in networking or some other field, you will be expected to make presentations to audiences with a wide range of interests and abilities.

Select a lesson/topic, with instructor approval, from the *Internetworking Fundamentals* course, or the review topics in this lesson, for a class presentation.

Prepare a one-page summary of the chosen lesson/topic. The summary may **not** be more than one page, typed, single-spaced.

Prepare a five-minute oral presentation for an audience of (choose one) professionals, laypersons, students, sales persons, research and development personnel, or other group of your choice. Establish the appropriate style and tone for your target audience.

Identify the needs of your target audience by preparing a list of questions you think they will want answered. Try to answer these questions as part of your presentation. Be prepared to answer additional questions from your audience after your presentation.

A visual aid(s) must accompany your presentation. The visual might be in the form of charts and graphs, computer presentation, reading materials, video, etc.

If anyone in your group knows sign language, ask them to sign the presentation.

Have each member of the audience complete presentation evaluation forms. Critique your own performance by completing a self-evaluation form. Do not be too harsh on yourself or others. This is among the first of many presentations you will give in your career. As the year progresses, it is expected that your presentations/evaluations will improve.

## Presentation Evaluation Form

**<u>Directions:</u>** When completing the evaluation form, rate the presenter as one of the following:

- 4-Exceptional
- 3-Talented
- 2-Satisfactory
- 1-Inexperienced
- 0-Unprepared

After each section, defend your rating with constructive comments that are positive and helpful. Remember that these same classmates will rate you.

**<u>Presentation of Content</u>:** Facts are complete, accurate, and show evidence of thorough research, analysis, and synthesis. Suitable for particular audience, correct grammar.

4 3 2 1 0 Score ______

Comments:

**<u>Organization:</u>** Stays focused on topic and does not digress. Ideas flow in a logical fashion. Fully prepared for the presentation.

4 3 2 1 0 Score ______

Comments:

**<u>Presentation Style:</u>** Enthusiastic, professional, interesting, relaxed. Easy to hear and understand, makes frequent eye contact, keeps within the time limit.

4 3 2 1 0 Score ______

Comments:

**<u>Visual Aids:</u>** Creative use of materials. Aids are appropriate to both the topic and audience, are well organized and add to the overall presentation, show attention to detail.

4 3 2 1 0 Score ______

Comments:

**<u>Question and Answer Period:</u>** Well informed and prepared to answer all questions. Gives thorough answers and address the specific questions asked. Ability to acknowledge the fact that s/he does not have all of the answers.

4 3 2 1 0 Score ______

Comments:

**<u>Effort:</u>** In an organization, people are valued for their individual talents. Not all individuals are expert presenters, however they are still valued employees. A successful business understands and needs the diversity people bring to a company. With this in mind, rate the effort the project shows.

4 3 2 1 0 Score ______

Comments:

**Total Score ____________**

**Rubric: Suggested Evaluation Criteria and Weightings:**

| **Criteria** | **%** | **Your Score** |
|---|---|---|
| Complete, concise, accurate one-page summary of selected topic | 10 | |
| Clear, concise, and organized, technical presentation. Delivered in terms understandable and appropriate to the audience | 20 | |
| List of questions prepared prior to presentation | 10 | |
| Relevancy, accuracy, and creativity of selected visual aid(s) | 10 | |
| Overall poise, demonstrating self-assurance and confidence during presentation and question/answer period | 15 | |
| Impartial, fair-minded evaluation of self and other participants | 15 | |
| Average of performance evaluation scores | 10 | |
| Attentive, active audience participation | 10 | |
| **TOTAL** | **100** | |

## Stretch Yourself

**Materials Needed:**

- Classroom Network
- Basic Sniffer software
- Internet Connection (optional)


**Mapping Your LAN**

In this activity, you will use the Sniffer Basic software to map the components and workstations connected to your Classroom LAN. In Lesson 1-1, you configured the LAN, and in Lesson 1-2, you configured your student workstations, a printer, and a network router. Once you have discovered all of the devices connected to your LAN you will print a diagram which maps the devices, their logical names, physical addresses, and IP addresses.

You will then run Sniffer Basic, capture packets for analysis, and observe the 350T Switch flooding, forwarding, and building its forwarding table. You must have at least three people in your group to complete all tasks.

This activity is broken down into the following five parts. Place a check in the box on the right to indicate when you have completed each part.

**Part 1: Install and Run Sniffer Basic Software**

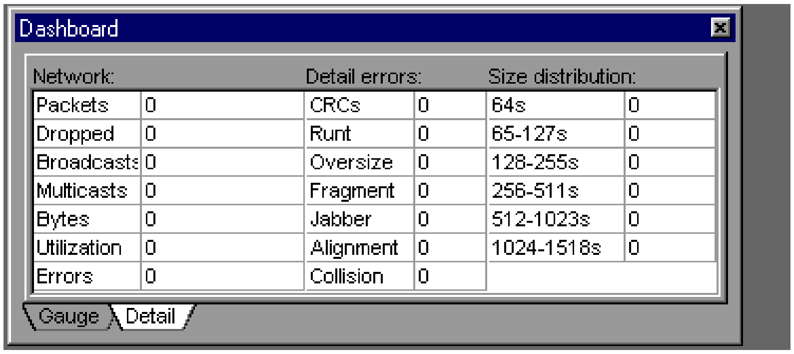
If the software is not already installed on your workstation, do so at this time. Be sure you obtain the software License Serial Number from your instructor.

**Part 2: Review of Sniffer Software**

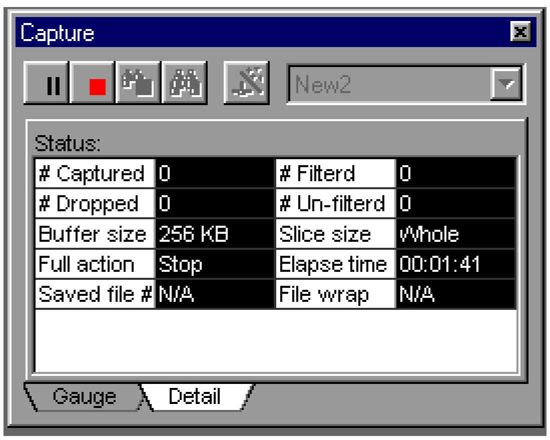
Follow these steps to learn about the basic features and capabilities of the Sniffer Basic product and to discover how it can be a powerful tool for looking into a network:

1. Maximize the Sniffer Basic window. Find the Icon Bar in the Sniffer Basic window.

2. Click on the ninth icon from the left. It is the one with the pink circle inside a black circle.  It will display the Dashboard:



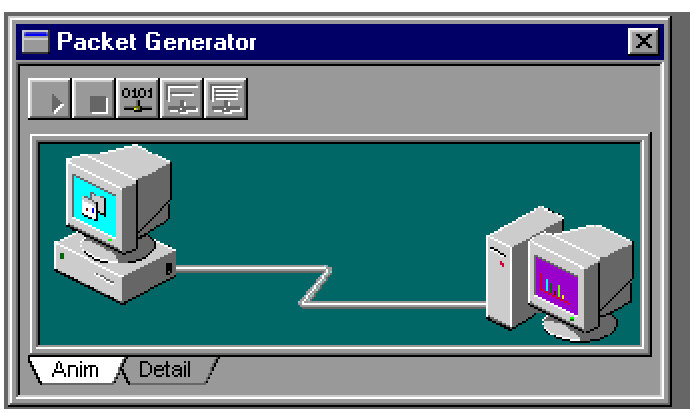

3. Click the tab marked Detail.




You can see the numbers, which show detailed information on the packets that have been transmitted.

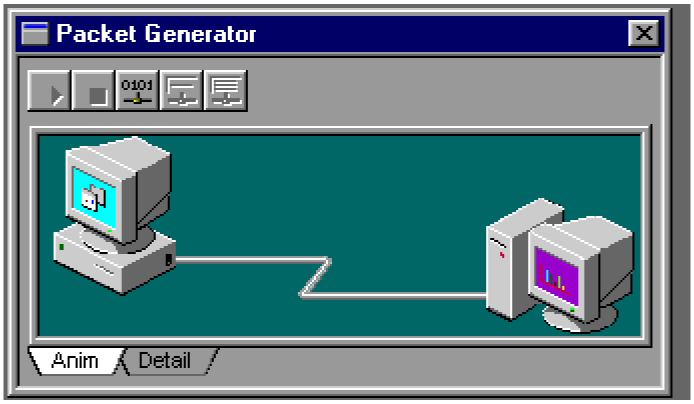
4. Click the X in the upper right corner of the Capture Tool to put it away.

5. Click the next Icon  to view the Packet Generator Tool.

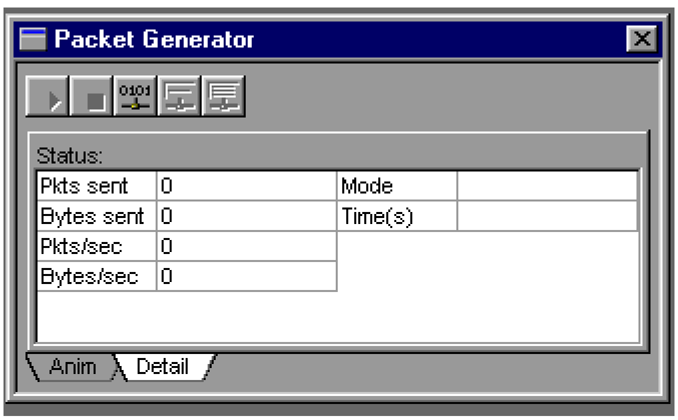



This tool lets you design and automatically generate traffic on your network. You will use this tool later for simulation and testing.

6. Click the next Icon  to view the Packet Generator Tool.

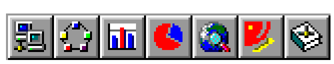



This tool lets you design and automatically generate traffic on your network. We will use this tool later for simulation and testing.




You can see statistics on the traffic generated by the Packet Generator Tool.

7. Click the X in the upper right corner of Packet Generator Tool, to put it away.



The other icons in the toolbar start an interesting set of other tools. You will be using most of them with other activities during this course.

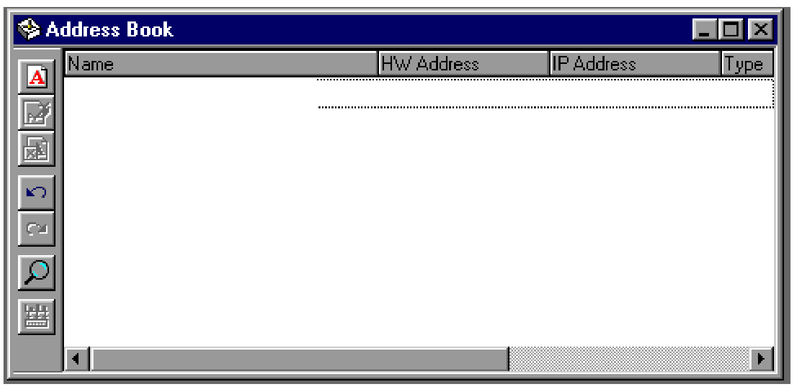
**Part 3: Discover your Network**

Follow these steps to use the Sniffer Basic software to discover, view, and analyze the devices connected to your classroom network. You should be able to identify each device connected to the network and print out listings.

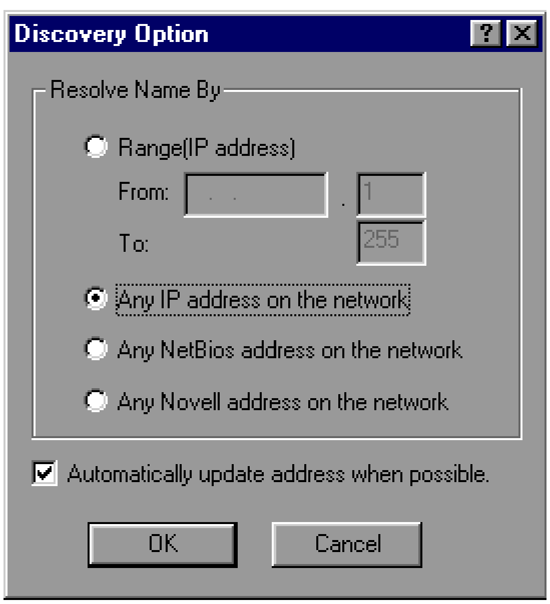
With the Sniffer software running and maximized on your desktop, find the Icon Bar in the Sniffer window.

1. Click on the icon all the way to the right. It is the one with the **X** on a book. 

   It will display the Sniffer Address Book.




2. Now click your right mouse button and select the choice for Auto Discovery, and you will see this dialog box:

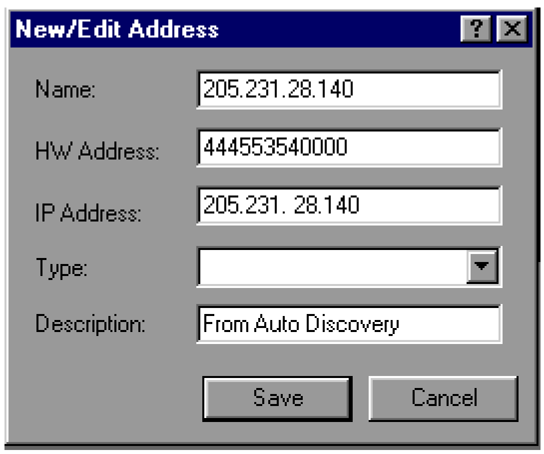



3. You will want to select the choice for Any IP address on the network. Then click OK to discover the devices on your network.

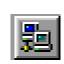
The Sniffer will now go out and try to identify each device on the network. Be patient, it may take a few minutes to discover all the devices on your network.

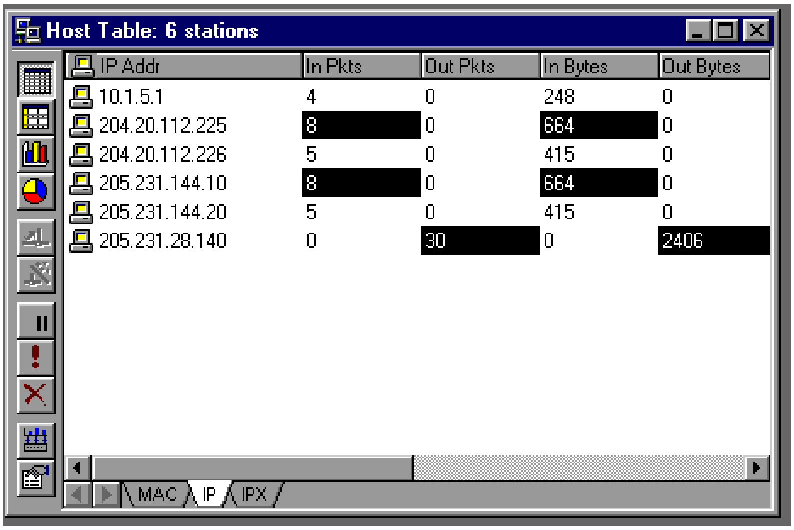

4. After the Sniffer finishes discovering devices on your network, you should look at the listing to determine whether all the devices that you know are physically present are listed. Make a list.

   You should also double-click on each device in the list and choose the Type selection to enter the type of device.



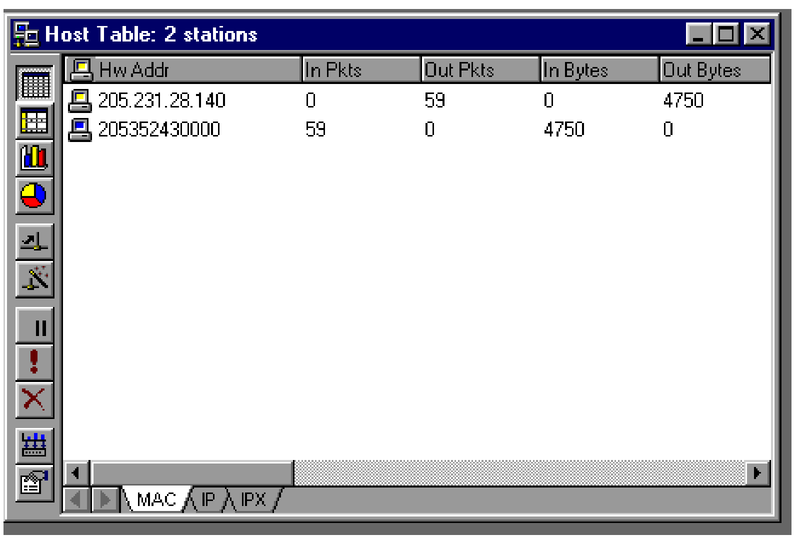

   You may need to check individual computer IP addresses using *WINIPCFG* to figure out which device is which. When you identify each device in the list, you can replace "From Auto Discovery" with the actual description (e.g., Laser Printer 1, or Computer 3, or Router A).

5. Now, click on the icon for the traffic Host Table.  Make sure IP tab is selected at the bottom of the screen.




In the Host Table, you will find real time statistics on traffic between your devices. Print this page.

If you select the MAC tab at the bottom, you will be able to view the hardware MAC addresses for each device.




6. Compare the MAC addresses with those you cataloged in Lesson 1-1. Print this page.

   Review the printouts of devices listed on the IP and MAC page. Use this information to complete your address book.

   You will use your list of missing devices in the next part of this activity.

**Part 4: Fixing Workstation Problems**

Based on the techniques you learned in prior courses, you should work through a set of troubleshooting steps to connect any workstations or devices that did not appear in the Address Book during your network discovery.

Document your work so you can explain the steps you took to the class. When you have completed your troubleshooting, run Sniffer again to be sure the entire network is operational.

**Part 5:**

1. Read all of these directions *before* you proceed. Start Sniffer Basic to capture packets during this activity for analysis purposes. Save, print, annotate, and add pertinent Sniffer files to your portfolio.
2. Connect your workstation to a port on the switch. Observe and record what happens.
3. When first attached to a network, a switch builds a forwarding table.
   - Once plugged in, how long does it take for the switch to build its forwarding table?
   - How long does it take for the switch to rebuild its forwarding table?
   - Why is this information important for a network manager?
4. This step will require group cooperation and coordination of the steps so that Sniffer Basic can capture evidence of flooding before the switch has an opportunity to build its new forwarding table. Be sure you have data ready to send to the new device.

   Coordinate and preplan with partners before completing this step. Have one member of the group connect a new workstation device to a port on the switch. Other members should send data to the new workstation device immediately, before the switch has a chance to build its new forwarding table.
5. Capture evidence of flooding with Sniffer software.
6. Write a one-page report on your findings for your portfolio.
7. Participate in class discussion about the results of this activity.

**Rubric: Suggested Evaluation Criteria and Weightings:**

| **Criteria** | **%** | **Your Score** |
|---|---|---|
| Accurate answers to lab questions and annotations on Sniffer Basic packet capture printouts that indicate a thorough understanding of concepts covered in this lab | 20 | |
| Printouts with MAC and IP addresses and portfolio entries complete | 20 | |
| Identify any devices which are not properly connected to the network and successfully troubleshoot the problems | 25 | |
| Student worked independently to diagnose and correct problem and referred to prior Lesson materials as necessary | 20 | |
| Active participation in group/class activity/discussion | 15 | |
| **Other** | | |
| **TOTAL** | **100** | |

## Network Wizards

**Materials Needed:**

- Classroom Network
- Optivity software

**Part 1: Generating and Using HP OpenView Maps**

During this lab, you will become familiar with the applications used to document a network. These applications, including CCC, Flat Network View, Segment View, RouterMan, NodalView, and Expanded View, help to determine if all network devices have been discovered.

In Part 1 of this lab, you run HP OpenView Autodiscovery and generate HP OpenView static maps. Then, you will learn how to launch some of the main Optivity applications from HP OpenView maps.

Part 1 of the lab is required in order to launch Optivity applications from OpenView network maps. This allows Optivity applications to run independently, without depending on the HP OpenView discovery process.

Keep a log of your experiences during this activity and prepare a summary of your experiences and an insightful analysis of how a network manager might use this software to help improve network performance.

Submit this summary to your instructor and place in portfolio.

1. Identify which networks you want to discover

   HP OpenView lets you control the extent of network discovery. You can decide just how much, or how little, of the network you want to look at. In very large and complex networks, you can use several network management stations to manage different portions of the network.

   In this step, you will tell the Open View software exactly which subnetworks, in your classroom network, you would like to include in your initial discovery process. In the discovery process, you may choose to discover only some of your subnets, or all of them.

   Once again, keep a record of your experiences and prepare a summary for your portfolio.

   a. Before you begin, you should verify that the computer you will be running the Open View software on is properly connected. To do that, ping your classroom network default router and your team's NMM. You can refer to the diagram your teacher gave you for these numbers.

**Note**

If any ping test fails, determine the cause of the problem and correct it with help from your instructor, BEFORE you begin this activity.

---

b. Double–click the Optivity 7.0 icon to open Optivity and HP OpenView. Sign on as **manager** with no password.

c. On the Autodiscovery menu, choose Configure, then drag right and choose Discovery Networks.

   The Configure Discovery Networks window opens.

d. In the IP Subnet Mask box, type the subnet mask provided by your instructor.

e. In the IP Default Gateway box, type the IP address of the classroom network's default router.

f. Enter the read community string, if necessary.

g. In the Networks field, type the number of an IP subnetwork and the Subnet Mask you want to discover in your classroom network and click Add.

   Repeat this step for each IP subnetwork your instructor asks you to discover in the classroom network.

   These entries will determine which subnetworks will be discovered.

h. Click OK.

2. Run OpenView Autodiscovery to discover your network.

   In this step, you will run the OpenView discovery process, which creates a map file containing information about the manageable devices on your network.

   a. Pull down the Autodiscovery menu and choose Discover, then choose Discover Routers.

   b. Click Yes when the system prompts you to start router discovery.

      The system takes a short time to query the default router and to obtain the ARP cache for each router in the classroom network. No notification is generated when the process is complete.

   c. To view the progress of the discovery process, pull down the Autodiscovery menu and choose Discover, then choose Discovery Manager.

   d. After discovery is complete, close the Discovery Manager window.

The Discovery Manager window shows devices discovered and the current status of the HP OpenView discovery process. If not all devices have been discovered, click the Start Discovery button.

3. View and Lay out OpenView maps.

   Now that you have successfully completed discovery of your network, you will be able to display your network maps, by following the instructions in this step.

   a. Pull down the Autodiscovery menu and choose Layout, then choose Do Basic Layout.

   b. Select Yes when the system asks whether or not to proceed.

      OpenView takes a short time to generate maps from the map file. Two types of maps will be generated. The ALLNETS map provides the Internetwork View for the entire discovered network. A separate network map is created for each subnetwork you have identified. These network maps are linked to each subnetwork icon on the Internetwork View.

      If the system does not find an Advanced NMM for each subnetwork selected for discovery, the Select Flat Network to Describe window opens.

   c. To identify manually a representative NMM, click the Describe button in the Select Flat Network to Describe window. In the window that opens, enter the IP address and other information provided by your instructor for your representative NMM.

   d. Once you have your ALLNETS map displayed you can verify the manageability of each subnetwork on the map, by clicking the right mouse button on each network icon and choosing Describe.

      The Describe Device window opens. It contains information about the NMM devices in that subnetwork.

   e. Verify the host name, IP address, management type (SNMP or Ping), and the community strings.

   f. All NMMs and router agents should use the SNMP management type. The subnetwork icon should change to a cloud and be green.

   g. Click Cancel.

4. Save the OpenView database.

   Network maps are stored in an OpenView database. You have to save the current map file if you want to update the OpenView database. In this step, you will save your current map file.

   a. On the File menu, choose Save As.
   b. In the File Name box, type **c:\opt\bin\[teamname]**.

      where `[teamname]` is your team's name.
   c. Click OK to save the new file name.

5. View the Layout of HPOV Network Maps.

   In this step, we will use the HP OpenView Network Maps to display and describe the equipment associated with each subnet.

   a. Double-click on your subnetwork.
   b. The map that appears contains all of the discovered devices in the subnet you have chosen.

**Part 2: Configuring and Using CCC**

In Part 1 of the lab, you used HP Open View to discover, map, and add node information to the map database. You also opened Optivity Views from HP OpenView maps.

Now, in Part 2 of this lab, you will learn to open Optivity CCC, run Autodiscovery, and configure the CCC options. In this part you will learn to:

- Run Campus Command Center
- Identify equipment type and agent level
- Set CCC Preferences
- Add a new custom folder to CCC
- Add a single new device to CCC
- Save your configuration file for CCC

CCC has a convenient toolbar for its important application components. You can find out what each icon means by holding the right mouse button over the icon.

1. Run Campus Command Center.

   a. On the HPOV main menu, choose the Applications pull down menu.

b. On the Applications pull down menu, choose Campus Command Center.

c. Once Campus Command Center is active, run the Autodiscovery process as outlined in the previous activity.

2. Identify equipment type and agent level.

   a. From the CCC folders panel, click on the Hubs folder.

   b. In the Contents panel, choose your hub and double-click on it.

   c. The Summary tab of the Attributes panel should now display information for the hub that you have chosen.

3. Set CCC Preferences.

   There are two preference menus for use within CCC. One is for hubs and the other for folders.

   - Select a hub and preferences allow you to select Verbose mode, Open Last Configuration, and Auto Sort.
   - Select a folder and preferences allow changes to thresholds and poll intervals for the Attributes Health tab.

   You will now set some CCC preferences. Let's say you want to see more details on the objects within your folders:

   a. In the Contents panel, select a hub.

   b. Pull down the CCC Option menu and choose Preferences.

   c. Select the Verbose box on the window that appears.

      CCC displays the number of objects within each folder.

   d. Click the Open Last Configuration button.

      The saved configuration will be used each time you open CCC. By default Autosort contents is selected.

   e. Click OK.

      The CCC folders now display the number of objects within each folder.

**Note**

The three panel sizes may be adjusted by clicking and dragging the dividers. It may be necessary to move the divider between the Contents and Attributes panels to see everything in the Attributes panel.

---

4. Add a new custom folder to CCC.

   a. Click the New Folder button on the CCC toolbar or pull down the Edit menu and choose New Folder.

   b. Type your team's name for the name of the folder and click OK. Confirm that a new folder is created.

   c. Click the Hubs folder.

   d. In the Contents panel, hold down the [Ctrl] key, click and hold the left mouse button on your team's NMM, and drag the icon to the new folder. Open the new folder to confirm that the hub has been copied to the new location.

      The hub remains in its original location and is copied to the new folder. Be careful, if you drag and drop a device without the [Ctrl] key, the device is moved, rather than copied.

5. Add a single new device to CCC.

   a. With the custom folder you just created selected, click the Add button in the toolbar or choose Add Device from the Edit menu.

      The Add Device window opens.

   b. In the Device Type field, select a print server icon for the device.

   c. In the Host Name field, type your team's name.

   d. Enter the network address of your team's management station.

   e. Change the selection button for Management Type to Ping.

   f. Click Save.

      An icon with the device's IP address is added to the appropriate folder.

      Click Yes to enter the device into the database. Select Servers from the Folders panel and highlight the new device and ping it to confirm connectivity.

6. Save your configuration file for CCC.

   a. On the File menu, choose Save As.

   b. Enter your team's name followed by the extension .CCC for the name of the CCC configuration file. The configuration file is saved in the directory `[driveid]:\OPT\BIN`.

   c. Click OK.

**Rubric: Suggested Evaluation Criteria and Weighting**

| Criteria | % | Your Score |
|---|---|---|
| Successful completion of activity | 15 | |
| Accurately follows directions | 15 | |
| Complete, accurate responses to lab activity questions | 15 | |
| Complete summary of experiences and an insightful analysis of how a network manager might use this software to help improve network performance. | 20 | |
| Summary included in portfolio | 15 | |
| Participation and cooperative teamwork during activity | 20 | |
| **Other** | | |
| **TOTAL** | **100** | |

# Summary

## Lesson 3: Network Protocols

In this unit, you learned to do the following:

- Explain how switches use Layer 2 protocols to segment a network and obtain hardware addresses
- Describe TCP/IP protocols and their relationship to switching
- Explain the function of BootP, TFTP, and ARP
- Describe DHCP and explain its importance in networking
- Differentiate between RIP and OSPF

*Name*______________________

## Review Questions Name______________________

### Lesson 3: Network Protocols

Directions: Select the best answer.

1. Which address(es) below would be valid on a WAN network?
   a. Physical MAC Address
   b. Logical static IP address
   c. Logical dynamic IP address
   d. All of the above
2. Which of the following statements about addresses is false.
   a. The MAC address always remains the same
   b. Layer 4 protocols identify source and destination MAC addresses on a LAN
   c. The logical address uniquely identifies a network device and its network segment
   d. If a computer is moved to another network, the IP address changes
3. Which of the following statements about transport layer protocols (TCP) is false?
   a. TCP provides end-to-end reliable delivery
   b. TCP can lose data if it is coming too fast
   c. TCP makes sure that all packets are received error-free
   d. TCP ensures that all packets are in the right order
   e. TCP ensures that no packet is duplicated

4. Which of the following statements about IP addressing is true?
    a. An IP address is not necessary to transmit data over the Internet
    b. When a network connects to the Internet, each device must have a unique IP address obtained from an Internet authority
    c. The second part of the IP address identifies the network where the device is located
    d. The first part of the IP address identifies the device on that network
5. From your reading on dynamic and static IP addresses, which of the following is false.
    a. DHCP is an extension of BootP to dynamically assign an IP address from a centrally managed DHCP server
    b. Dynamic addressing eliminates tying up IP addresses that are not in use
    c. DHCP and BootP both notify a host of its IP address when connecting to a network
    d. A server can have a dynamic IP address
6. Which of the following statements about TFTP is false?
    a. Trivial File Transfer protocol (TFTP) is a protocol within the User Datagram Protocol (UDP)
    b. TFTP exists in programmable read-only memory (PROM) of a device
    c. TFTP contains only two types of TFTP packets: RRQ and Data
    d. TFTP can be used with BootP for installing a remote network operating system
    e. TFTP gets BootP data back and forth between the boot server and the client device
7. Which of the following statements is false.
    a. When information is built into hardware, it is always slower than software
    b. Until recently switches were layer 2 devices and not capable of routing across networks
    c. Switching routers (also called layer 3 switches) and are faster than routers because some of the routing protocols are now built into the hardware

*Name*________________________

d. Routers and switching routers use layer 3 routing protocols to move data traffic from one network to another by the fastest route(s) available

8. Switching routers can route across similar and dissimilar network segments creating VLANs, an abbreviation for:

   a. Virtual Logical Area Networks

   b. Virtual Local Area Networks

   c. Vector Local Area Networks

9. From your reading on the RIP routing protocol, which of the following statements is false?

   a. Routing Information Protocol (RIP) calculates the distance between two points over a variety of routes, selecting the shortest path

   b. Information on paths is stored and updated in a database table for the routing device

   c. This database information is shared with other devices

   d. RIP is an older routing protocols and works well for larger network

10. From your reading on the OSPF routing protocol, which of the following statements is false?

    a. Open Shortest Path First (OSPF) is a link state protocol solution that does not use distance-vector algorithms

    b. OSPF does not just examine the distance between two points, but takes into consideration Type of Service (TOS) such as speed of data transmission and fault tolerance of a line

    c. To be more efficient, OSPF limits itself to IP protocol to construct routing tables

    d. OSPF breaks networks into sections called areas, defined by traffic patterns, not geographical locations

    e. Areas limit down-time, routing table edits, and other parameters to just one area of a network

## Scoring

| Criteria | % | Your Score |
|---|---|---|
| Explain how switches use layer 2 protocols to segment a network and obtain hardware addresses | 20 | |
| Describe TCP/IP protocols and their relationship to switching | 20 | |
| Explain the function of BootP, TFTP, and ARP | 20 | |
| Describe DHCP and explain its importance in networking. | 20 | |
| Differentiate between RIP and OSPF | 20 | |
| **TOTAL** | **100** | |
| **Try It Out:** The Windows 95/98 Utilities | **100** | |
| **Stretch Yourself:** Building a MAC Forwarding Table | **100** | |
| **Network Wizards:** Comparing Switches | **100** | |
| **Review** | **100** | |
| **FINAL TOTAL** | **500** | |

## Resources:


Aschermann, Robert (1998). *MCSE Networking Essentials for Dummies*. IDG Books Worldwide, Inc. Foster City, California.

Black, Darryl P. (1999). *Building Switched Networks: Multilayer Switching, QoS, IP Multicast, Network Policy, and Service Level Agreements.* Addison-Wesley, Reading, Massachusetts.

Bert, Glen (1998). *MCSE Networking Essentials: Next Generation Training Second Edition*. New Riders Publishing, Indianapolis, Indiana.

Casad, Joe, et al (1997). *MSCE TestPrep Networking Essentials.* New Riders Publishing, Indianapolis, Indiana.

Chellis, James; Perkins, Charles; & Strebe, Matthew (1997). *MCSE Networking Essentials Study Guide.* Sybex Inc., Alameda, California.

Computing and Communications Services Office, University of Illinois at Urbana-Champaign (1999). *Network Administrator's Survival Handbook.* Available: www.ntx2.cso.uiuc.edu/nas/network_administrator.htm [1999, May 13].

Groth, David. Bergersen, Ben. Catura-Houser, Tim (1999). *Network+ Study Guide.* Sybex Inc., Alameda, California.

Nortel Networks (1998). *Internetworking Fundamentals: Student Guide* Bay Networks Inc. Billerica, Massachusetts.

Nortel Networks (1999). *NetKnowledge: Internetworking Fundamentals.* Nortel Networks, Billerica, Massachusetts.

Nortel Networks (1999). *NetKnowledge: Routing.* Nortel Networks, Billerica, Massachusetts.

Palmer, Michael J. (1998). *Hands-On Networking Essentials with Projects,* Course Technology, Inc. Cambridge, Massachusetts.

Trinity College Dublin, Computer Science Department, Networks & Telecommunications Research Group (1999). *The OSI Reference Model.* Available: ganges.cs.tcd.ie/4ba2/index.html [1999, May 13].