Spolufinancováno
z programu Evropské unie
Erasmus+

NETWORK ADMIN

COVERAGE:

I Network Interface

II Network Cabling

III File and Print Sharing

IV TCP/IP Network Model

V IP Addressing

VI Ethernet Switching

VII LAN Topologies

NETWORK ADMIN

NETWORK INTERFACE

Objectives:
Install a network interface card (NIC) into a personal computer (PC).

Step-by-Step Instructions:

The more inexpensive the NIC, usually the more problems you will have installing it. It usually applies more to the software side of networking but there are also problems on the hardware side.

Do not buy cheap NICs unless you want to experiment or have had good experiences with a certain brand of NICs before.

1. Unplug the PC power cord from the wall or outlet.

Warning
Do not attempt to install a NIC into a powered PC. Electrocution is a bad experience.

2. Remove the cover from the PC using screwdrivers or nut drivers as the case may be. Every PC is different so go slowly, don't force anything, and ask questions whenever needed.

3. Remove a cover plate from an available slot (usually a PCI slot) using a screwdriver.

4. Gently slide the NIC into the appropriate slot. You may have to rock it slightly forward and backward.

5. Attach the NIC with a screw to the case foundation.

6. Replace the cover.

7. Plug in the PC again.

8. You are now ready for the software portion of the installation, although this can vary. Sometimes the workstation will auto-sense a new NIC is installed and will take care of it automatically. Other times you will have to manually add the driver software.

NETWORK ADMIN

NETWORK CABLING

Objective:
Learn which type of network cable to use in which instance.

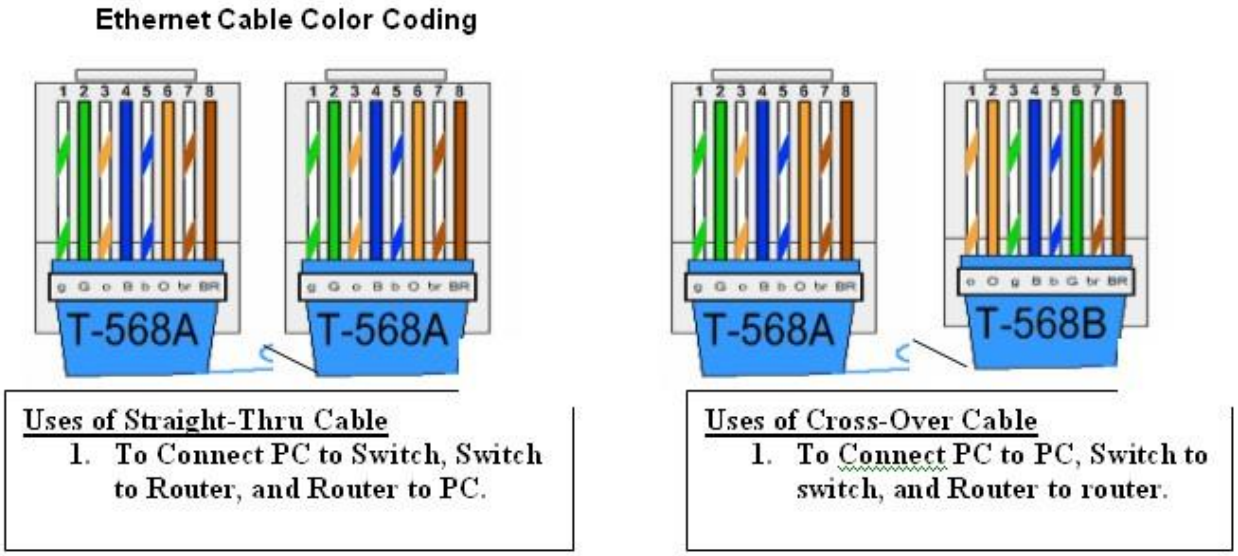
Background:

You will be putting together lots of networking equipments with plenty of cables during your networking career.

Knowing which cable to use and when will save you plenty of time, trouble, and embarrassment if you get it right from the start.

Some network administrators do not know a straight-through from a cross-over or a roll-over.

Wiring patterns have evolved from the telephone industry. The two most common wiring patterns are EIA/TIA 568A and EIA/TIA 568B (Electronics Industry Association / Telecommunications Industry Association).



NETWORK ADMIN

NETWORK CABLING

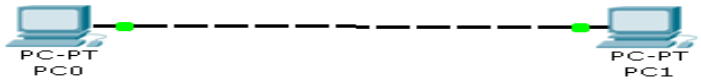
Wire Pin	T568A	T568B
1	striped Green	striped Orange
2	solid Green	solid Orange
3	striped Orange	striped Green
4	solid Blue	solid Blue
5	striped Blue	striped Blue
6	solid Orange	solid Green
7	striped Brown	striped Brown
8	solid Brown	solid Brown

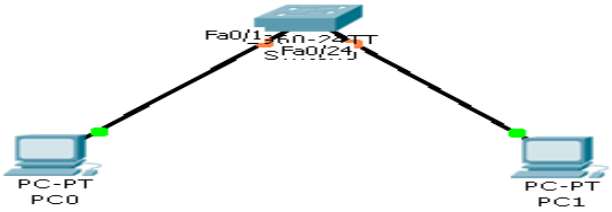
Straight-Through (ST): Used for connecting dissimilar devices (workstations to hubs, switches to routers, hubs to switches, etc.). The cables are wired with the same wiring pattern on each end.

Cross-over (XO): Used for connecting similar devices (workstations to workstations, switches to switches, hubs to hubs, etc). The cables are wired with different wiring patterns on each end.

Roll-over (RO): Used for connecting communication ports to other communication ports (workstation serial com ports to router console ports, etc). It does not matter which colors are used here as long as the pattern “rolls over” from one side to the other. Wires 12345678 roll-over to 87654321 on the other end.

In the following diagrams indicate which type of cable is used:

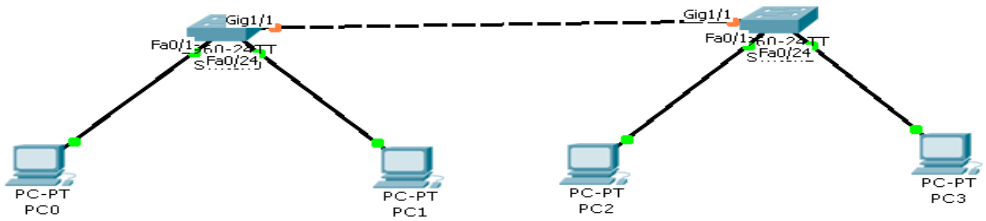


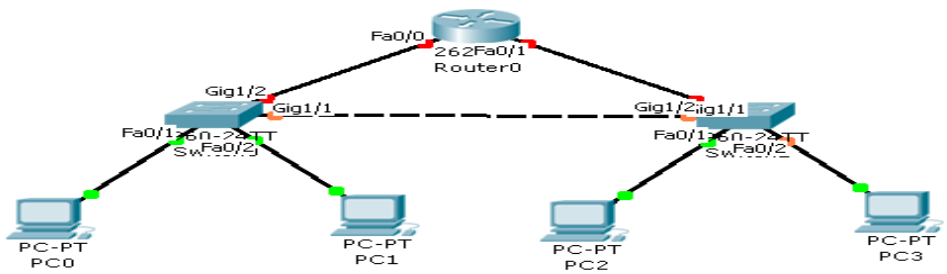


NETWORK ADMIN

NETWORK CABLING

In the following diagrams indicate which type of cable is used:



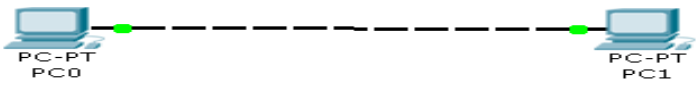


NETWORK ADMIN

FILE AND PRINT SHARING

Objective:
Set up two computers to communicate and share files.

Lab Diagram:



IP addresses: 192.168.1.1 192.168.1.2
Subnet Masks: 255.255.255.0 255.255.255.0
Gateway: 192.168.1.2 192.168.1.1

Step-By-Step Instructions:

1. Cable the lab as shown. Put one end of the crossover cable in the NIC on one computer and the other end in the NIC of the other computer. Make certain the LED lights up on

the NIC when the cable is plugged into both ends. If the lights do not turn on, then check to make sure you have a good crossover cable.

2. Change the TCP/IP settings on each computer.

3. Enable file and print sharing by right clicking the “network places” (just like you did for changing the TCP/IP settings. Click on the file and print sharing box.

4. Select the “pick box” for file sharing.” You can pick the one for print sharing if you have printers that need to be shared also. Re-boot your computer.

5. After your computer reboots you have to actually share some files. Otherwise you won’t see anything when you access the other computer. An easy way to enable file sharing is with the “my computer” icon on your desktop. Double-click on it and right click on the “C” drive and select sharing. Now file sharing can be accomplished.

6. If you only want to share a specific folder or document double click on the C drive to open it and then select the folder or document and pick sharing. On the other computer you should only see that folder or document.

NETWORK ADMIN

FILE AND PRINT SHARING

7. In either case you will be presented with a window for setting the parameters for the share. Create a name for the drive, folder, or document. You can allow full access, read only, or password-protected access to the drive, folder or document.

8. Once you are finished select “apply”, then “OK,” and you should be able to see the drive, folder, or document on the other computer.

Additional Activities:

1. Pick one computer to be the computer for your boss. The other will be the employee. Have only certain folders and documents sharable on the boss’s computer. Have all drives shared on the employee’s computer. Can your boss find out where you have been on the Internet?

2. Put a dollar sign ($) on the end of a shared file name and see what happens.

NETWORK ADMIN

TCP/IP NETWORK MODEL

The Internet was developed to provide a communication network that could continue to function in wartime.

TCP/IP is a network protocol ideal for the de-centralized concept of the Internet.

The U.S. Department of Defense created the TCP/IP Network Model, wanting information to get through every time, under any condition, from any one point to any other point.

The Internet has evolved in ways very different from those envisioned by its creators, but it is still based on the TCP/IP Network Model.

The TCP/IP Network Model has 4 Layers

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Network Access Layer

TCP/IP APPLICATION LAYER

Handles high-level protocols, and issues of representation, encoding, and dialog control.

Application Layer Protocols

1. HTTP – Hypertext Transfer Protocol is used by the World Wide Web to define how messages are formatted and transmitted, and what actions web servers and web browsers should take in response to web client requests.

2. TFTP – Trivial File Transfer Protocol is a connectionless service that uses the User Datagram Protocol (UDP) to transfer files between systems that support TFTP.

3. FTP – File Transfer Protocol is a connection-oriented service that uses the Transmission Control Protocol (TCP) to transfer files between systems that support FTP.

4. NFS – Network File System is a distributed file system protocol that allows remote file access across a network.

TCP/IP NETWORK MODEL

5. SMTP – Simple Mail Transport Protocol transmits email across computer networks.

ADVANCED NETWORKING

,

TCP/IP APPLICATION LAYER

6. SNMP – Simple Network Management Protocol provides monitoring and control of network devices, and on managing configurations, statistics collection, performance monitoring, and security.

7. DNS – Domain Name System translates domain names into their public IP addresses.

8. Telnet – provides remote access to another computer

TCP/IP TRANSPORT LAYER

Provides transport services from the source host to the destination host, segments and re-assembles applications into the same data stream between end points.

When using UDP, the Transport Layer transports data from source to destination.

When using TCP, the Transport Layer provides end-to-end control and reliability.

Transport Layer Services

1. Segmenting application data
2. Sending segments from one end device to another end device
3. Establishing end-to-end operation
4. Providing reliability

TCI/IP INTERNET LAYER

Sends packets from a device using the correct protocol and determines the best path from source to destination.

NETWORK ADMIN

TCP/IP NETWORK MODEL

Internet Layer Protocols

1. IP – Internet Protocol provides connectionless, best-effort delivery of packets.

2. ICMP – Internet Control Message Protocol provides control and messaging capabilities.

3. ARP – Address Resolution Protocol determines the MAC addresses for known IP addresses.

4. RARP- Reverse ARP determines the IP addresses for known MAC addresses.

IP Operations

1. Define a packet and its addressing scheme
2. Transfer data between the Internet Layer and the Network Access Layer
3. Route packets to remote hosts

TCP/IP NETWORK ACCESS LAYER

It is concerned with all the issues that a packet requires to make physical link to the network medium, also known as the Host-to-Network Layer.

Network Access Layer Operations

1. Map IP addresses to MAC addresses
2. Encapsulate packets into frames
3. Define the connection with the network medium

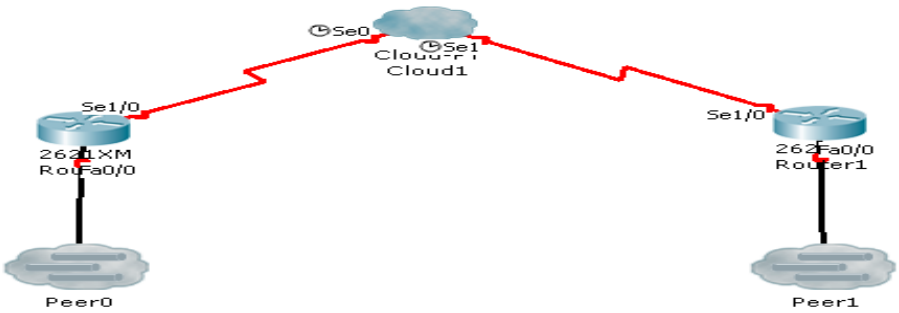
NETWORK ADMIN

TCP/IP NETWORK MODEL

TCP/IP Model Summary:

1. Application and Transport Layers are concerned with protocols.
2. Internet and Network Access Layers are concerned with networks.

Below is an Inter-Network of two LANs connected by two routers and a communications carrier, over a large geographical area.



Users on both LANs can communicate with each other even without being directly connected to one another.

LANs do not scale beyond a certain number of stations and beyond a certain geographic separation. A third-party communications carrier, usually a telephone company (telco) is needed to connect LANs across large distances.

Each router interface connects to a different LAN.

Characteristics of an Inter-Network

1. Scalable in the number of networks and computers attached
2. Can handle the transport of data across large distances
3. Flexible to constant technological innovations
4. Can adjust to dynamic conditions on the network
5. Cost-effective
6. Allows anytime, anywhere access to information for anyone

NETWORK ADMIN

IP ADDRESSING

For any two systems to communicate they must be able to identify and locate each other.

There must be a way to identify individual hosts and the network that they belong to.

The combination of host identification and network identification creates a unique address for each device on the network.

A computer might be connected to more than one network, this is done by having two network interface cards (NIC) each connected to different networks, and each having different network address and host address.

Inside the computer, the IP address is stored as a 32-bit sequence of 1s and 0s.

To make the IP address easier to use, it is written as four decimal numbers separated by dots, known as dotted-decimal notation.

Each part of an IP address is called an octet because it is made up of 8 binary digits.

Aside from easier to write and understand, dotted-decimal notation prevents transposition errors.

Every IP address has two parts, one part identifies the network to which the device or host is connected, and the second part identifies the particular host or device.

Each octet ranges from 0 to 255.

The subnet mask indicates the network portion and the host portion of an IP address.

IP ADDRESS CLASSES

	First Octet	Subnet Mask	Hosts per Network
Class A	0 – 127	255.0.0.0	16, 777, 216
Class B	128 – 191	255.255.0.0	65, 535
Class C	192 – 223	255.255.255.0	254

IP ADDRESSING

RESERVED IP ADDRESSES

1. Network Address – the first IP address that is used to identify the network where the hosts or devices belong to.
2. Broadcast Address – the last IP address that is used to send packets to all hosts and devices on a network.

PRIVATE IP ADDRESSES

Class A	10.x.x.x
Class B	172.16.x.x up to 172.31.x.x
Class C	192.168.x.x

Private addresses are not routed on the Internet, they are immediately discarded by routers on the Internet.

Connecting a network to the Internet using private addresses require translating the private addresses to public addresses, this network address translation is performed by routers.

SUBNETTING

Is the method of dividing a network into smaller networks or subnets in order to reduce the size of the broadcast domain.

A broadcast is an area in a network that exists so that a device can send a message to every device on the network.

* Reducing the broadcast domain improves network performance.

Example: Divide a Class C network 192.168.0.0 into three subnets, the first subnet has 4 hosts, second subnet 8 hosts, third subnet 16 hosts.

Answer:
first subnet 192.168.1.0 / 255.255.255.248
second subnet 192.168.2.0 / 255.255.255.240
third subnet 192.168.3.0 / 255.255.255.224

IP ADDRESSING

SUBNET MASKING

Is the process of adjusting the subnet mask according to the required number of hosts or required number of subnets.

Example: What is the subnet mask for a Class C network that has 4 hosts?

Solution: 4 host addresses + 2 (for the network address and broadcast address)
= 6 IP addresses

8 is the nearest power-of-2 number to 6

128 64 32 16 8 4 2 1
1 1 1 1 1 0 0 0

248 is the decimal equivalent of 1 1 1 1 1 0 0 0

Answer: The subnet mask for a Class C network that has 4 hosts is 255.255.255.248

Example: What is the subnet mask for a Class C network that has 4 subnets?

Solution: 4 subnets 2 4 8 16 32 64 x x
1 1 0 0 0 0 0 0

192 is the decimal equivalent of 1 1 0 0 0 0 0 0

Answer: The subnet mask for a Class C network that has 4 subnets is 255.255.255.192

STATIC IP ADDRESSING

- Each host or device IP Address is manually configured.
- Required by host or device that is referenced by other hosts or devices.
- Prone to duplication of IP addresses.

NETWORK ADMIN

IP ADDRESSING

DYNAMIC IP ADDRESSING

- Each host or device IP Address is automatically assigned by a DHCP Server

ADDRESS RESOLUTION

- In TCP/IP communications, a datagram on a LAN must contain both the destination MAC address and the destination IP address

ADDRESS RESOLUTION PROTOCOL (ARP)

- Allows a host to store a map of MAC addresses with their corresponding IP addresses
- The MAC-IP map, called an ARP Table, is a section of RAM maintained automatically on each device (PC> arp –a)

DEFAULT GATEWAY

- Is the IP Address of the router interface that connects to the LAN on which the host is located

PACKETS and FRAMES

- A packet contains end-to-end addressing (IP), works across broadcast domains
- A frame contains local addressing (MAC), works within a broadcast domain

NETWORK ADMIN

ETHERNET SWITCHING

A switch is a multi-port bridge that provides a concentration point for the connection of computers, routers, and other switches.

A bridge is a device designed to create two LAN segments, each of which is a separate collision domain.

The purpose of a bridge is to filter traffic on a LAN to keep local traffic local, yet allow connectivity to other segments for traffic that is directed there.

To filter traffic, bridges build tables of all MAC addresses located on a network segment and other networks, and map them to associated ports.

Bridging Process

1. As a frame comes along the network medium, a bridge compares the destination MAC address carried by the frame to MAC addresses contained on its table.

2. If the source MAC address is unknown, the bridge creates a new entry in the MAC Address Table with the source port.

3. If the bridge determines that the destination MAC address of the frame is from the same segment as the source, it does not forward the frame to other segments of the network. This process is called filtering.

4. By performing filtering, bridges can reduce the amount of traffic between network segments through elimination of un-necessary forwarding.

5. If the bridge determines that the destination MAC address of the frame is not from the same segment as the source, it forwards the frame to the appropriate segment.

6. If the destination MAC address is unknown, the bridge broadcasts the frame to all devices on the network except the one on which it was received. This process is known as flooding.

A bridge has only two ports, and divides a collision domain into 2 parts.

All decisions made by a bridge are based on MAC addresses, therefore, a bridge divides a collision domain but not a broadcast domain.

NETWORK ADMIN

ETHERNET SWITCHING

No matter how many bridges are on a network they all share the same broadcast address space.

All segments in a bridge environment are considered to be in the same broadcast domain.

Latency

Is the time a frame takes to travel from the source to its destination on the network, also known as propagation delay.

Causes of Latency

1. Speed limitation that signals can travel through the media
2. Circuit delays on processing the signal along the path
3. Software delays on decisions the system must make to implement protocols and switching
4. Frame content
5. Determining destination

Switching Modes

1. Store and Forward
    - Frames are completely processed and checked for errors before forwarding to the appropriate port or interface
    - Frames are also buffered until network resources are available for forwarding

2. Fast Forward
    - Immediately forwards a frame after receiving the destination MAC address

3. Fragment-free
    - Filters out collision fragments, which are smaller than 64 bytes

NETWORK ADMIN

ETHERNET SWITCHING

Switch Functions

1. Address Learning
    - The source MAC address of a frame is entered into the MAC Address Table

2. Forwarding and Filtering
    - The switch looks at the destination MAC address of a frame and finds the exit interface in the MAC Address Table

3. Loop Avoidance
    - Spanning Tree Protocol (STP) is used to prevent network loops while still permitting redundancy

Spanning Tree Protocol (STP)

STP is a link management protocol that is used to maintain a loop-free network.

A loop-free topology is accomplished when the switch recognizes a loop in the topology and blocks one or more redundant ports automatically.

When the network topology changes, the switches running STP will reconfigure their ports to avoid loss of connectivity.

Three Steps to a Loop-free Network Topology

1. Elect a Root Switch
    - Only one switch can act as a root in a given network
    - All ports on the root switch become designated ports
    - Designated ports are in the forwarding state, they can send and receive network traffic

2. Select Root Ports on non-Root Switches
    - The root port is the lowest-cost path from the non-root switch to the root switch
    - Root ports are in the forwarding state

NETWORK ADMIN

ETHERNET SWITCHING

Three Steps to a Loop-free Network Topology

3. Select the Designated Port on each Segment
    - Only one designated port is established per each segment
    - Designated ports are selected on non-root switches based on the lowest-cost path to the root switch
    - Non-designated ports on non-root switches discards network traffic, also known as blocking ports

A Converged Switch Network would have:

1. One root switch per network
2. One root port per non-root switch
3. One designated port per segment
4. All non-designated ports are blocked

Electing the Root Switch

1. Every two seconds, switches send to all other switches messages that allow the forming of loop-free topology. These messages are called BPDUs (Bridge Protocol Data Unit)

2. Even blocked ports receive BPDUs, which ensures that if a path or a device fails a new spanning tree can be calculated

3. Included in the BPDU is the Bridge ID (BID) consisting of a bridge priority number (that defaults to 32768) and the switch's base MAC address

4. Upon startup, the switch sends a BPDU indicating that it is the root switch

5. As the switch receives BPDUs of other switches, it compares their BIDs. Every time it receives a lower BID, it sends the lower BID as the root switch

NETWORK ADMIN

ETHERNET SWITCHING

STP States

1. Blocking
    - No frames forwarded, BPDUs received

2. Listening
    - No frames forwarded, listens for frames

3. Learning
    - No frames forwarded, learns addresses

4. Forwarding
    - Frames forwarded, learns addresses

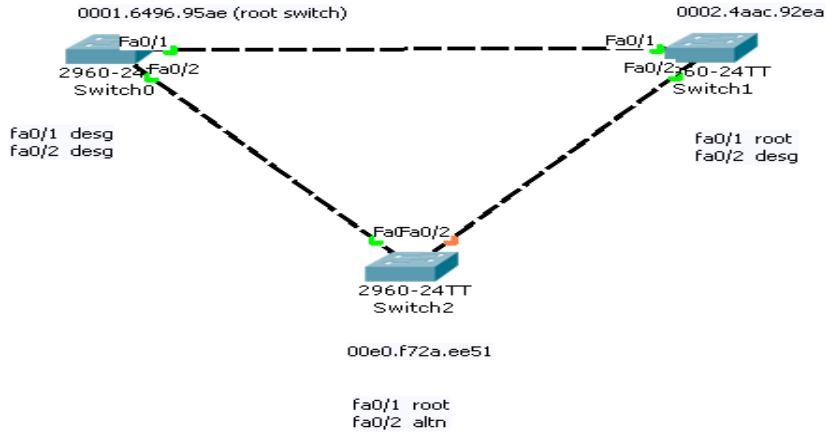
5. Disabled
    - No frames forwarded, no BPDUs received

Spanning Tree Path Cost

Link Speed	Path Cost
10 GBPS	2
1 GBPS	4
100 MBPS	19
10 MBPS	100

NETWORK ADMIN

ETHERNET SWITCHING



Spanning Tree Process

1. All three switches have default priority values (32768), therefore, the switch with the lowest MAC address becomes the root switch (Sw0)

2. Sw0 then sets its ports as designated ports (forwarding)

3. Sw0 and Sw1 have to select their root ports

4. Each segment should have one designated port. For the Sw1-Sw2 segment, the designated port is fa0/2 of Sw1 and the alternate port is fa0/2 of Sw2 (non-designated blocking port)

NETWORK ADMIN

LAN TOPOLOGIES

Objective:
Learn more about the topologies used in networking.

Background:

A **bus topology** has all devices connected to a central backbone cable with terminating resistors on each end of the central backbone cable. This really is not used too much any more since one computer, connector, or cable segment can cause the entire network to go down.

Bus topologies typically used coaxial cabling (50 to 62 ohm, not the 75 ohm for TV). Commonly known as thicknet and thinnet LANs.

A **star topology** has all networking devices connected to a central device. The most widely used network topology.

Star topologies usually use category 5 or 5e UTP or STP cabling.

Ring topologies have every device connected to exactly two other devices. Ring topologies are most commonly used in fiber-optic networks.

Most large networks fall into the general category called **hybrid topology** which means some of this topology type and some of that topology type.

There are all kinds of other topologies that are just extreme versions of the three basic topologies:

Extended Star: Two or more star networks connected together with a backbone cable.

Mesh or Full-mesh: Every computer or networking device connected to every other computer or networking device (used primarily in frame relay networks).

Tree: Like a hard drive structure with folders and documents.

Irregular: Free-form networking.

Cellular: Exacting cells with a networking device at the middle. Nodes and networking device use wireless networking.

NETWORK ADMIN

QUIZZES

Quiz 1: Changing MAC/IP Addresses and Network Devices

1. Bridges make low-level, simple comparisons and decisions about whether or not to forward traffic on a network. True or False?

2. If the bridge determines that the destination MAC address carried by a data packet is part of the same network segment as the source, it does not forward the data to other segments of the network. True or False?

3. Bridges solve the problem of too much traffic on a network by dividing the network into segments and filtering traffic based on the MAC address. True or False?

4. When a bridge forwards data on a network, it determines precisely what segment of the network the data will be forwarded to. True or False?

5. When a bridge makes a decision about whether to forward data on a network or not, it uses only the IP address carried by the data in its header. True or False?

6. Describe what a frame is.

7. At which layer of the TCP/IP model does routing occur?

8. At which layer of the TCP/IP model does bridging occur?

9. At which layer of the TCP/IP model is the MAC address located?

10. If a workstation is moved within a network, then what will happen to its MAC and IP addresses?

11. If a workstation is moved from one network to another network, then what will happen to its MAC and IP addresses?

12. Routers pass packets between _____?

NETWORK ADMIN

QUIZZES

Quiz 1: Changing MAC/IP addresses and Network devices

13. Which part of the IP address does a router ignore during path determination?

14. Which type of address is included in an IP header?

Quiz 2: IP Addresses

Are the following statements TRUE or FALSE?

1. If a device on network A is moved to network B, its IP address will change.

2. IP addresses are used to identify a machine on a network and the network to which it is attached.

3. Each network connected to the Internet has a unique network number.

4. The network portion of every IP address is assigned by the local network administrator.

5. How many bits are in an IP address?

6. How many bytes are in an IP address?

7. What is the minimum decimal value in an octet?

8. What is the maximum decimal value in a byte?

9. How many bits are in a byte?

10. How many bytes are in a MAC address?

NETWORK ADMIN

QUIZZES

Quiz 3: Classes of IP Addresses

1. To which class of IP address would the IP address of 197.22.103.221 belong?

2. In a class A network using an IP addressing scheme, the first sixteen bits are used for the network part of the address, and the last two octets are reserved for the host part of the address. True or False?

3. To what class of network would the IP address 144.26.108.15 belong?

4. To what class of network would the IP address 18.12.245.10, belong?

5. In the IP address 190.233.21.12, how many octets have been assigned by the NIC?

6. In the IP address 88.224.73.201, how many octets could be assigned locally by the network administrator?

7. Describe a class B network.

8. A class C network address would have all binary 0s in its final octet. True or False?

9. A class B network address would have all binary 0s in its final two octets. True or False?

10. Give an example of a class C network address.

11. Describe a class C network.

12. Describe a class A network.

13. Give an example of a class C IP address.

14. How many octets have been assigned by InterNIC in a class C network?

15. If you have a class A IP address, how many bytes have been assigned to you for your hosts?

NETWORK ADMIN

QUIZZES

Quiz 4: Binary to Decimal Conversions

1. 11111111 convert to decimal

2. 197.15.22.31 convert to binary

3. 197.15.22.127 convert to binary

4. 11111111.11111111.11111110.00000000 convert to dotted decimal

5. 01010101 convert to decimal

6. 01111110 convert to decimal

7. 00010000 convert to decimal

8. 01100110 convert to decimal

9. 00001000 convert to decimal

10. 17 convert to binary

11. 128 convert to binary

12. 220 convert to binary

13. 240 convert to binary

14. 191 convert to binary

NETWORK ADMIN

QUIZZES

Quiz 5: Broadcast and Subnet addresses

1. Describe a broadcast.

2. Give an example of a class C broadcast address.

3. In a class C subnet address up to six bits can be borrowed from the host field. True or False?

4. Give a valid class B broadcast address with no subnets

5. What is the broadcast address of 198.64.74.x /27?

6. Give a valid class C subnet number.

7. Give a valid class B subnet broadcast address.

8. Which type of IP address can borrow one bit from the last octet to create subnets?

9. Describe the address 147.30.74.1

Quiz 6: Possible vs. Useable Subnetting

Are the following statements TRUE or FALSE?

1. Subnet addresses are assigned locally.

2. Subnet addresses include only a network number and a host number.

3. Each time the number of bits borrowed from an eight bit octet decreases, the decimal value representing that octet in the subnet mask increases by a power of two

4. How many possible subnets can be created if four bits are borrowed from the host field?

NETWORK ADMIN

QUIZZES

Quiz 6: Possible vs. Useable Subnetting

5. How many possible subnetworks can be created if five bits are borrowed from the host field?

6. How many possible subnetworks can be created if six are borrowed from the host field?

7. How many actual subnets can be created if four bits are borrowed from the host field?

8. How many actual subnetworks can be created if five bits are borrowed from the host field?

9. How many possible subnetworks can be created if six are borrowed from the host field?

10. On a class C network with three bits borrowed for subnets to which subnetwork would the IP subnet and host range 01100001 belong?

11. How would the subnetwork 01100001 field for a Class C IP address with six useable subnets be expressed in binary numbers?

12. How would the third useable subnet range of a Class C IP address with eight possible subnets be expressed in decimal numbers?

13. How would the decimal number 220 be expressed as a binary number written as an octet?

14. How would the sixth possible subnetwork field of a Class C IP address be expressed in binary numbers?

15. To what subnetwork on a Class C network with three bits for a subnet would a fourth octet expressed as 10101101 belong?

16. How would the host field be expressed in binary numbers of a Class C IP address which has 6 useable subnets for host number 13?

NETWORK ADMIN

QUIZZES

Quiz 6: Possible vs. Useable Subnetting

17. What is the maximum number of bits that can be borrowed in a Class C network?

18. What is the maximum number of bits that can be borrowed in a Class B network?

19. If two bits are borrowed from the host field of a Class C network, then how many possible subnetworks can be created?

20. If four bits are borrowed from the host field of a Class B network, then how many subnetworks can be created?

21. If four bits are borrowed from the host field of a Class B network, then how many possible hosts per subnetwork can be created?

22. If two bits are borrowed from the host field of a Class C network, then how many possible hosts per subnetwork can be created?

23. If we have 4 possible subnets in our network then how many bits have been borrowed from the host field?

24. If we have 4 possible subnets in our network then what will be the range of binary host field numbers for the first subnetwork?

25. If we have 4 possible subnets in our network then what decimal value would be assigned to an octet expressed as 01011011?

26. If we have 2 possible subnets in our network then what would be the binary subnetwork field number for the decimal host number expressed as .196?

27. In a network with two bits borrowed for subnets, what would the binary host field number be for the decimal host number expressed as .49?

NETWORK ADMIN

QUIZZES

Quiz 7: Subnet Masking

1. How would the subnet mask 255.255.255.0 be represented in dotted binary notation?

2. If only seven bits are borrowed in a Class B network then what would the subnet mask be in dotted decimal notation?

3. What would the subnet mask be in dotted decimal notation if only five bits were borrowed from the third octet in a class B address?

4. What would the subnet mask be in dotted decimal notation if only one bit were borrowed from the third octet in a Class A address?

5. Subnet masks tell devices which part of an address is the network number including the subnet and which part is the host. True or False?

6. Subnet masks are 16 bits long and are divided into two octets. True or False?

7. Subnet masks have all 0s in the network and subnetwork portions of their addresses. True or False?

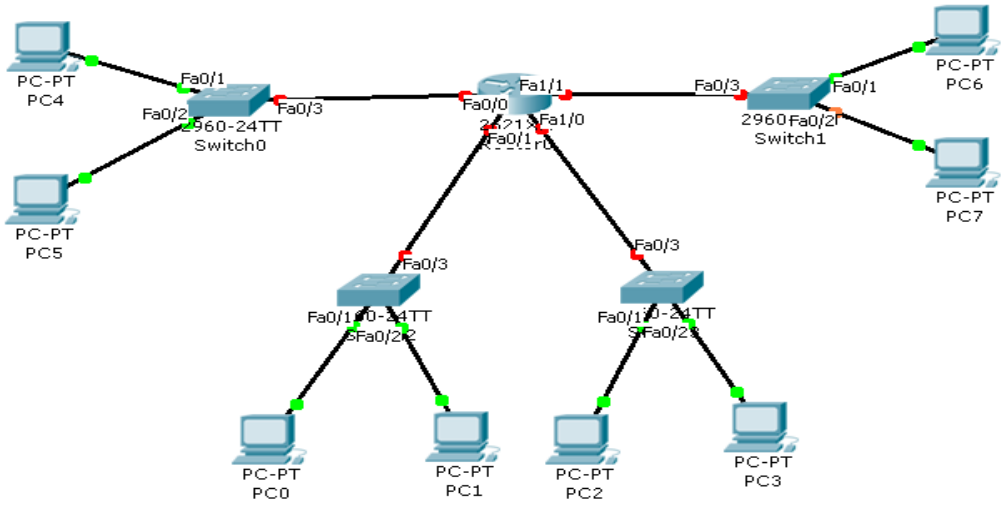
8. Binary bits in the subnet mask are used to represent _____.

9. What will the use of subnets do regarding the amount of broadcast traffic?

NETWORK ADMIN

QUIZZES

Quiz 8: Router Functions



NET1 – PC4 and PC5 NET3 – PC2 and PC3
NET2 – PC0 and PC1 NET4 – PC6 and PC7

1. In the topology above, if device PC4 is sending data to device PC0, out of what port will the router send the data?

2. In the topology above, how many IP addresses does the router have?

3. In the topology, if device PC5 wants to send data to device PC4, will the router forward the data to Network 4?

4. How many ports does the router in this topology have?