Quick Notes - LAN

What is carrier sense multiple access collision detect (CSMA/CD)?
CSMA/CD describes the Ethernet access method. In CSMA/CD, many stations can transmit on the same cable, and no station has priority over any other. Before a station transmits, it listens on the wire to make sure no other station is transmitting. If no other station is transmitting, the station transmits across the wire. CSMA/CD is all about devices taking turns using the wire.

What are MAC addresses?
For computers to identify each other on the data link layer, they need a MAC address (hardware address). All devices on a LAN must have a unique MAC address. A MAC address is a 48-bit (six octet) address burned into a network interface card. The first three octets (24 bits) of the MAC address indicate the vendor that manufactured the card. This is called the Organization Unique Identifier (OUI). The last three octets of the MAC address are the unique host address. An example of a MAC address is 00-80-C6-E7-9C-EF.

What are the three types of LAN traffic?
The three types of LAN traffic are:
Unicasts
Broadcasts
Multicasts

What are unicast frames?
Unicast frames are the most common type of LAN traffic. A unicast frame is a frame intended for only one host. In unicast frames, the only station that processes the frame is the station that has its own MAC address in the destination portion of the packet.

What are broadcast frames?
Broadcast frames are frames intended for everyone. Stations view broadcast frames as public service announcements. All stations receive and process broadcast frames. In large networks, broadcasts can bring the network to a crawl, because every computer must process them.

What is the destination address of broadcast frames?
The destination address of broadcast frames (Layer 2 broadcast addresses) is FF-FF-FF-FF-FF-FF, or all 1s in binary.

What are multicast frames?
Multicast frames address a group of devices that have a common interest. These frames allow the source to send only one copy of the frame on the network even though it is intended for several stations. Only stations that have a card that is configured to receive multicast frames process them. All other stations discard multicast frames.

What devices can you use to segment a LAN at Layer 1, Layer 2, and Layer 3?
Three devices you can use to segment a LAN are:
Hubs/repeaters (Layer 1)
Bridges/switches (Layer 2) - physical addresses
Routers (Layer 3) - logical addresses

What happens when you segment the network with hubs/repeaters?
Because hubs and repeaters operate at the physical layer of the OSI model, segmenting a network with these devices appears as an extension to the physical cable. Hubs and repeaters are transparent to devices. They are unintelligent devices. All devices that connect to a hub/repeater share the same bandwidth. Hubs/repeaters create a single broadcast and collision domain.

What is the advantage of segmenting a network with bridges/switches?
Bridges/switches operate at Layer 2 of the OSI model and filter by MAC address. Each port on a bridge/switch provides full-dedicated bandwidth and creates a single collision domain. Because bridges/switches operate at Layer 2 of the OSI model, they cannot filter broadcasts, and they create a single broadcast domain. For the CCNA test, remember that switches create more collision domains and fewer collisions.

What is the difference between bridges and switches?
Bridges and switches function the same way; the only difference is in how they are implemented. Bridges are implemented by software and usually have a couple of network ports. Switches are implemented in hardware by ASIC chips and have many ports.

What are the advantages and disadvantages of segmenting the LAN with routers?
An advantage of segmenting the LAN with routers is that each interface on a router creates a single broadcast and collision domain. Routers operate at Layer 3 of the OSI model and do not propagate broadcasts. Some disadvantages are that routers are not transparent and are implemented in software, thus introducing latency in the network.

What is the Maximum Transmission Unit (MTU) for an Ethernet frame?
1500 bytes is the MTU for an Ethernet frame. You will notice that some publications state that the MTU for Ethernet is 1518 bytes. This is correct also. But what is the true answer? The MTU for Ethernet, including the header, source and destination address, data, and CRC is 1518 bytes. The MTU for the data portion of the frame is 1500 bytes.

What three major functions do Layer 2 switches provide?
The three major functions that Layer 2 switches provide are

Address learning
Packet forwarding/filtering
Loop avoidance by spanning tree

What are some advantages of switches?
Some advantages of switches are as follows:
They increase available network bandwidth.
They reduce the number of users per segment.
They provide dedicated bandwidth to each segment.
Transparent bridging (switching) provides five bridging functions to determine what to do when it receives a frame.

What are these five processes?
The five processes are:
Learning
Flooding
Filtering
Forwarding
Aging

In transparent bridging, what is the learning process?
The first process a bridge goes through when it is powered on is the learning process. The MAC address table on the bridge contains no entries, and the bridge goes through the learning process to record all workstations on every interface. In the learning process, the bridge records the source MAC address and source port number in the MAC address table every time it sees a frame.

In transparent bridging, what is the flooding process?
When a bridge is first turned on, it has no MAC address in its table. When a switch receives a unicast frame, it knows the source address and port from which the unicast frame came, but no entry exists in its table for the destination address. This is called an unknown unicast frame. When a switch receives an unknown unicast frame, it sends the frame out all forwarding interfaces on the bridge except the interface that received the frame. This process is the flooding process.

In transparent bridging, what is the filtering process?
The filtering process occurs when the source and destination addresses reside on the same interface on the bridge. Because the bridge does not need to forward a frame in which the destination and source addresses reside on the same interface, it filters the frame and discards it.

In transparent bridging, what is the forwarding process?
The forwarding process occurs when a switch receives a unicast frame and has an entry of the destination address in its MAC table. The switch then forwards the frame to the interface where that destination address resides.

In transparent bridging, what occurs during the aging process?
Every time a bridge learns a source address, it time-stamps the entry. When the bridge sees a frame from this source, it updates the time stamp. If the bridge does not hear from the source for a specific amount of time (called the aging timer), the bridge deletes the entry from its MAC address table. This process is the aging process.

What is the default aging time in transparent bridges?
The default aging timer is 5 minutes.

What is the Spanning-Tree Protocol (STP)?
STP is a loop-prevention bridge-to-bridge protocol. Its main purpose is to dynamically maintain a loop-free network. It does this by sending out Bridge Protocol Data Units (BPDUs), discovering any loops in the topology, and blocking one or more redundant links.

How does STP maintain a loop-free network?
STP maintains a loop-free network by
Electing a root bridge
Electing a root port on each nonroot bridge
Electing designated ports
Putting in the blocking state any port that is not a root port or designated port

What two key concepts does STP calculation use to create a loop-free topology?
The two key concepts that STP uses to calculate a loop-free topology are
Bridge ID (BID)
Path cost

In spanning tree, what is a Bridge ID (BID)?
A BID is an 8-byte field that is composed of the bridge's 6-byte MAC address and a 2-byte bridge priority.

What is the default bridge priority in a Bridge ID for all Cisco switches?
32,768

In spanning tree, what is path cost?
Path cost is a calculation to determine the link's bandwidth. It is a value assigned to each port that is based on the port's speed.

What is the spanning tree path cost for each of the following?
10 Mbps
100 Mbps
1 Gbps
The path costs are as follows:
10 Mbps - 100
100 Mbps - 19
1 Gbps - 4

When calculating a loop-free environment, what four-step decision sequence does spanning tree use to determine what will be the root bridge and which ports will forward or block?

The four-step decision sequence that spanning tree uses to determine the root bridge and which port will forward is as follows:

Step 1. The lowest root BID

Step 2. The lowest path cost to the root bridge

Step 3. The lowest sender BID

Step 4. The lowest port ID

How do bridges pass spanning tree information between themselves?

Bridges pass STP information using special frame called Bridge Protocol Data Units (BPDUs).

How often do bridges send BPDUs out active ports?

The default time that bridges send BPDUs out active ports is 2 seconds.

Note: All ports on a switch listen for BPDUs in case there is a topology change.

In STP, how is a root bridge elected?

In STP, the bridge with the lowest BID is elected the root bridge. All ports on the root bridge are placed in the forwarding state and are called designated ports.

Note: The BID is a 6-byte field that is composed of a default priority (32,768) and a MAC address. Because all Cisco switches use the default priority, the switch with the lowest MAC address is elected the root bridge. As a rule of thumb, lower will always win in spanning tree.

After bridges elect the root bridge, what do they do next?

After electing the root bridge, switches elect root ports. A root port is the port on nonroot bridges that is closest to the root bridge. Every nonroot bridge must select one root port.

How do nonroot bridges decide which port they will elect as a root port?

Nonroot bridges use root path cost to determine which port will be the root port. Root path cost is the cumulative cost of all links to the root bridge. The port with the lowest root path cost is elected the bridge's root port and is placed in the forwarding state.

What is the difference between path cost and root path cost?

Path cost is the value assigned to each port. It is added to BPDUs received on that port to calculate the root path cost. Root path cost is defined as the cumulative cost to the root bridge. In a BPDU, this is the value transmitted in the cost field. In a bridge, this value is calculated by adding the receiving port's path cost to the value contained in the BPDU.

If a nonroot bridge has two redundant ports with the same root path cost, how does the bridge choose which port will be the root port?

If a nonroot bridge has redundant ports with the same root path cost, the deciding factor is the port with the lowest port ID (port number).

After the root bridge and root ports are selected, the last step in spanning tree is to elect designated ports. How do bridges elect designated ports?
In spanning tree, each segment in a bridged network has one designated port. This port is a single port that both sends and receives traffic to and from that segment and the root bridge. All other ports are placed in a blocking state. This ensures that only one port on any segment can send and receive traffic to and from the root bridge, ensuring a loop-free topology. The bridge containing the designated port for a segment is called the designated bridge for that segment. Designated ports are chosen based on cumulative root path cost to the root bridge.
Note: Every active port on the root bridge becomes a designated port.

If a bridge is faced with a tie in electing designated ports, how does it decide which port will be the designated port?
In the event of a tie, STP uses the four-step decision process discussed in Question 30. It first looks for the BPDU with the lowest BID; this is always the root bridge. If the switch is not the root bridge, it moves to the next step: the BPDU with the lowest path cost to the root bridge. If both paths are equal, STP looks for the BPDU with the lowest sender BID. If these are equal, STP uses the link with the lowest port ID as the final tiebreaker.

What are the four spanning tree port states?
The four spanning tree port states are
Blocking
Listening
Learning
Forwarding
Remember that root and designated ports forward traffic and that nondesignated ports block traffic but still listen for BPDUs.
Important note: There is another port state - Disabled - (No frames forwarded, no BPDUs heard). If it shows up in the answer options - select it along with the others.

What is the STP blocking state?
When a switch starts, all ports are in the blocking state. This is to prevent any loops in the network. If there is a better path to the root bridge, the port remains in the blocked state. Ports in the blocked state cannot send or receive traffic, but they can receive BPDUs.

What is the STP listening state?
Ports transition from a blocked state to a listening state. In this state, no user data is passed. The port only listens for BPDUs. After listening for 15 seconds (if the bridge does not find a better path), the port moves to the next state, the learning state.

What is the STP learning state?
In the STP learning state, no user data is being passed. The port quietly builds its bridging table. The default time in the learning state is 15 seconds.

What is the STP forwarding state?
After the default time in the learning state is up, the port moves to the forwarding state. In the forwarding state, the port sends and receives data.

What is STP forward delay?
The forward delay is the time it takes for a port to move from the listening state to the learning state or from the learning state to the forwarding state. The default time is 30 seconds.

What is the hello time in STP timers?
The hello time is the time interval between the sending of BPDUs. The default time is 2 seconds.

What is the Max Age timer?
The Max Age timer is how long a bridge stores a BPDU before discarding it. The default time is 20 seconds (ten missed hello intervals).

What is the default time a port takes to transition from the blocking state to the forwarding state?
The default time a port takes to transition from the blocking state to the forwarding state is 50 seconds: 20 seconds for Max Age, 15 seconds for listening, and 15 seconds for learning.

What does STP do when it detects a topology change in the network due to a bridge or link failure?
If spanning tree detects a change in the network due to a bridge or link failure, at least one bridge interface changes from the blocking state to the forwarding state, or vice versa.

Quick Notes - WAN

The three WAN connection types available are leased lines, circuit-switched, and packet-switched. Define the differences between each connection type.
Leased lines are dedicated point-to-point lines that provide a single preestablished WAN communication path from the customer's network to the remote network. Leased lines are usually employed over synchronous connections. They are generally expensive and are always up. Circuit-switched connections are dedicated for only the duration of the call. The telephone system and ISDN are examples of circuit-switched networks. Packet-switched connections use virtual circuits (VCs) to provide end-to-end connectivity. Packet-switched connections are similar to leased lines, except that the line is shared by other customers. A packet knows how to reach its destination by programming of switches. Frame Relay is an example of a packet-switched connection.

Define customer premises equipment (CPE), and give an example.
CPE is equipment that is located on the customer's (or subscriber's) premises. It is equipment owned by the customer or equipment leased by the service provider to the customer. An example is your router.

What is the demarcation point (demarc)?
The demarc is the point where the CPE ends and the local loop begins. It is the last responsibility of the service provider and is usually an RJ-45 jack located close to the CPE. Think of the demarc as the boundary between the customer's wiring and the service provider's wiring.

What is the local loop?
The local loop is the physical cable that extends from the demarc to the central office.

Describe the central office (CO).
The CO is the telco switching facility that connects the customer to the provider's switching network. The CO is sometimes referred to as a point of presence. It is the point where the local loop gains access to the service provider's access lines.

What is the toll network?
All the telco switches, COs, and trunk lines inside the WAN provider's network are the toll network.

What are synchronous links?
Synchronous links have identical frequencies and contain individual characters encapsulated in control bits, called start/stop bits, that designate the beginning and end of each character. Synchronous links try to use the same speed as the other end of a serial link.

What are asynchronous links?

Asynchronous links send digital signals without timing. Asynchronous links agree on the same speed, but there is no check or adjustment of the rates if they are slightly different. Only 1 byte per transfer is sent.

List some typical Layer 2 encapsulation methods for WAN links.

. High-Level Data Link Control (HDLC)
· Point-to-Point Protocol (PPP)
· Serial Line Internet Protocol (SLIP)
· X.25/Link Access Procedure, Balanced (LAPB)
· Frame Relay· Asynchronous Transfer Mode (ATM)

Describe HDLC.

HDLC was derived from Synchronous Data Link Control (SDLC). It is the default encapsulation type on point-to-point dedicated links and circuit-switched connections between Cisco routers. It is an ISO-standard bit-oriented data-link protocol that encapsulates data on synchronous links. HDLC is a connection-oriented protocol that has very little overhead. HDLC lacks a protocol field and therefore cannot encapsulate multiple network layer protocols across the same link. Because of this, each vendor has its own method of identifying the network-layer protocol. Cisco offers a propriety version of HDLC that uses a type field that acts as a protocol field, making it possible for multiple network-layer protocols to share the same link.

By default, Cisco uses HDLC as its default encapsulation method across synchronous lines (point-to-point links). If a serial line uses a different encapsulation protocol, how do you change it back to HDLC?

To change a serial line back to HDLC, use the following interface command on the serial interface you want to change: Router(config-if)#encapsulation hdlc

What is the Point-to-Point Protocol (PPP)?

PPP is an industry-standard protocol that provides router-to-router or router-to-host connections over synchronous and asynchronous links. It can be used to connect to other vendors' equipment. It works with several network-layer protocols, such as IP and IPX. PPP provides authentication through PAP or CHAP.

Describe X.25/LAPB.

X.25/LAPB is an ITU-T standard that has a tremendous amount of overhead because of its strict timeout and windowing techniques. LAPB is the connection-oriented protocol used with X.25. It uses the ABM (Asynchronous Balance Mode) transfer mode. X.25/LAPB was used in the 1980s when WAN links were not as error-free as they are today. X.25 is a predecessor of Frame Relay. X.25 supports both switched and permanent virtual circuits.

What is Frame Relay?

An industry standard, Frame Relay is a switched data link layer protocol that uses virtual circuits to identify the traffic that belongs to certain routers. It

provides dynamic bandwidth allocation and congestion control.

How do you view the encapsulation type on a serial interface?

To view the encapsulation type on a serial interface, use the show interface serial interface-number command:

```
RouterB#show interface serial 0
Serial0 is up, line protocol is up Hardware is HD64570
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 00:00:00, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0 Queueing strategy:
weighted fair Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
9 packets input, 1730 bytes, 0 no buffer
Received 8 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
7 packets output, 1584 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 output buffer failures, 0 output buffers swapped out
5 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Quick Notes - INTERNETWORKING

What are the three layers of the Cisco Hierarchical Model?
The three layers of the Cisco Hierarchical Model are:1
The access layer
The distribution layer
The core layer

In the Cisco Hierarchical Model, what is the function of the access layer?
Sometimes referred to as the desktop layer, the access layer is the point at which users connect to the network through low-end switches. Some functions of the access layer include:
Connectivity into the distribution layer
Shared Bandwidth
MAC Address filtering (switching)
Segmentation

What is the function of the distribution layer in the Cisco Hierarchical Model?
The distribution layer is also known as the workgroup layer. It is the demarcation point between the access and core layers of the network. Its primary function is to provide routing, filtering, and WAN access. The distribution layer determines how packets access the core, so it is the layer at which to implement policy-based connectivity. Some functions include the following:
Collection point for access layer devices
Broadcast and multicast domain segmentation
Security and filtering services such as firewalls and access lists
Providing translation between different media types
Inter-VLAN routing

What is the role of the core layer in the Cisco Hierarchical Model?
The core layer is the backbone of the network. Its main function is to switch traffic as fast as possible. Therefore, it should not perform any filtering to slow down traffic.
The ISO's OSI Reference Model contains seven layers. What are they? Include the layer number and name of each layer in your answer.
The seven layers of the OSI model are as follows:
Layer 7 - Application layer
Layer 6 - Presentation layer
Layer 5 - Session layer
Layer 4 - Transport layer
Layer 3 - Network layer
Layer 2 - Data link layer
Layer 1 - Physical layer

What are some reasons that the industry uses a layered model?
Here are some reasons why the industry uses a layered model:

It encourages industry standardization by defining what functions occur at each level.
It allows vendors to modify or improve components at only one layer versus rewriting the whole protocol stack.
It helps interoperability by defining standards for the operations at each level.
It helps with troubleshooting.

What does the application layer (Layer 7) of the OSI model do, and what are some examples of this layer?
The application layer is the layer that is closest to the user. This means that this layer interacts directly with the software application. The application layer's main function is to identify and establish communication partners, determine resource availability, and synchronize communication. Some examples include the following:
TCP/IP applications such as Telnet, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), WWW, and HTTP.
OSI applications such as Virtual Terminal Protocol, File
Transfer, Access, and Management (FTAM), and Common Management Information Protocol (CMIP).

In the OSI model, what are the responsibilities of the presentation layer (Layer 6)? Give some examples of this layer.
Also known as the translator, the presentation layer provides coding and conversion functions to application layer data. This guarantees that the application layer on another system can read data transferred from the application layer of a different system. Some examples of the presentation layer are:
Compression, decompression, and encryption
JPEG, TIFF, GIFF, PICT, QuickTime, MPEG, and ASCII

What are the functions of the session layer (Layer 5)? Give some examples.
The session layer is responsible for creating, managing, and ending communication sessions between presentation layer entities. These sessions consist of service requests and responses that develop between applications located on different network devices. Some examples include SQL, RPC, NFS, X Window System, ZIP, NetBIOS names, and AppleTalk ASP.

What is the transport layer (Layer 4) responsible for? Give some examples of transport layer implementations.
The transport layer segments and reassembles data from upper-layer applications into data streams. It provides reliable data transmission to upper layers. End-to-end communications, flow control, multiplexing, error detection and correction, and virtual circuit management are typical transport layer functions. Some examples include TCP, UDP*, and SPX.
Note: watch out for end-to-end on communications on the exam! Transport layer.

* Error correction does not apply to UDP - connection-less - unreliable.....

What is flow control, and what are the three methods of implementing it?
Flow control is the method of controlling the rate at which a computer sends data, thus preventing network congestion. The three methods of implementing flow control are
Buffering
Congestion avoidance
Windowing
Almost certain to be on the exam.

Describe the function of the network layer (Layer 3), and give some examples of network layer implementations.
The network layer provides internetwork routing and logical network addresses. It defines how to transport traffic between devices that are not locally attached. The network layer also supports connection-oriented and connectionless service from higher-layer protocols. Routers operate at the network layer. IP, IPX, AppleTalk, and DDP are examples of network layer implementations.

Are network layer addresses physical or logical?
Network layer addresses are logical addresses specific to the network layer protocol being run on the network. Each network layer protocol has a different addressing scheme. They are usually hierarchical and define networks first and then host or devices on that network. An example of a network address is an IP address, which is a 32-bit address often expressed in decimal format. 192.168.0.1 is an example of an IP address in decimal format.

How do routers function at the network layer of the OSI model?
Routers learn, record, and maintain awareness of different networks. They decide the best path to these networks and maintain this information in a routing table. The routing table includes the following:
Network addresses, which are protocol-specific. If you are running more than one protocol, you have a network address for each protocol.
The interface the router uses to route a packet to a different network.
A metric, which is the distance to a remote network or the weight of the bandwidth, load, delay, and reliability of the path to the remote network.
Routers create broadcast domains. One interface on a router creates a single broadcast domain and collision domain. However, an interface on a switch creates only a single collision domain.

In addition to learning the remote network and providing a path to the network, what other functions do routers carry out?
Routers perform these tasks:
Routers, by default, do not forward broadcasts or multicasts.
Routers can perform bridging and routing functions.
If a router has multiple paths to a destination, it can determine the best path to the destination.
Routers forward traffic based on Layer 3 destination addresses.

Routers can connect Virtual LANs (VLANs).
Routers can provide quality of service for specified types of network traffic.

What is the responsibility of the data link layer (Layer 2)?
The data link layer provides functional and procedural means for connectionless mode among network entities, and for connection mode entities it provides the establishment, maintenance, and release of data link connections among network entities and for the transfer of data link service data units. The data link layer translates messages from the network layer into bits for the physical layer, and it enables the network layer to control the interconnection of data circuits within the physical layer. Its specifications define different network and protocol characteristics, including physical addressing, error notification, network topology, and sequencing of frames. Data link protocols provide the delivery across individual links and are concerned with the different media types, such as 802.2 and 802.3. The data link layer is responsible for putting 1s and 0s into a logical group. These 1s and 0s are then put on the physical wire. Some examples of data link layer implementations are IEEE 802.2/802.3, IEEE 802.5/802.2, packet trailer (for Ethernet, the FCS or CRC), FFDI, HDLC, and Frame Relay.

The IEEE defines what two sublayers of the data link layer?
The two sublayers of the data link layer are
The Logical Link Control (LLC) sublayer
The Media Access Control (MAC) sublayer
These two sublayers provide physical media independence.

For what is the LLC sublayer responsible?
The Logical Link Control (802.2) sublayer is responsible for identifying different network layer protocols and then encapsulating them to be transferred across the network. An LLC header tells the data link layer what to do with a packet after it is received.

What functions does the Media Access Control (MAC) sublayer provide?
The MAC sublayer specifies how data is placed and transported over the physical wire. The LLC layer communicates with the network layer, but the MAC layer communicates downward directly to the physical layer. Physical addressing (MAC addresses), network topologies, error notification, and delivery of frames are defined at this sublayer.

What are some network devices that operate at the data link layer?
Bridges and switches are network devices that operate at the data link layer. Both devices filter traffic by MAC addresses.

What is the function of the OSI model's physical layer (Layer 1)? Give some examples of physical layer implementations.
The physical layer defines the physical medium. It defines the media type, the

connector type, and the signaling type (baseband versus broadband). This includes voltage levels, physical data rates, and maximum cable lengths. The physical layer is responsible for converting frames into electronic bits of data, which are then sent or received across the physical medium. Twisted pair, coaxial cable, and fiber-optic cable operate at this level. Other implementations at this layer are repeaters/hubs, RJ-45.

The Ethernet and IEEE 802.3 standards define what three physical wiring standards that operate at 10 Mbps?

These physical wiring standards operate at 10 Mbps:
10Base2
10Base5
10BaseT

What are collision domains?

In Ethernet segments, devices connect to the same physical medium. Because of this, all devices receive all signals sent across the wire. If two devices send a packet at the same time, a collision occurs. In the event of a collision, the two devices run a backoff algorithm and resend the packet. The devices retransmit up to 15 times. The first station to detect a collision issues a jam signal. When a jam signal is sent from a workstation, it affects all of the machines on the segment, not just the two that collided; when the jam signal is on the wire, no workstations can transmit data. The more collisions that occur in a network, the slower it will be, because the devices will have to resend the packet. A collision domain defines a group of devices connected to the same physical medium.

What are broadcast domains?

A broadcast domain defines a group of devices that receive each others' broadcast messages. As with collisions, the more broadcasts that occur on the network, the slower your network will be. This is because every device that receives a broadcast must process it to see if the broadcast is intended for it.

What devices are used to break up collision and broadcast domains?

Switches and bridges are used to break up collision domains. They create more collision domains and fewer collisions. Routers are used to break up broadcast domains. They create more broadcast domains and smaller broadcast areas.

How do the different layers of the OSI model communicate with each other?

Each layer of the OSI model can communicate only with the layer above it, below it, and parallel to it (a peer layer). For example, the presentation layer can communicate with only the application layer, session layer, and presentation layer on the machine it is communicating with. These layers communicate with each other using protocol data units (PDUs). These PDUs control information that is added to the user data at each layer of the model. This information resides in fields called headers (the front of the data field) and trailers (the end of the data field).

What is data encapsulation?

A PDU can include different information as it goes up or down the OSI model. It is given a different name according to the information it is carrying (the layer it is

at). When the transport layer receives upper layer data, it adds a TCP header to the data; this is called a segment. The segment is then passed to the network layer, and an IP header is added; thus, the data becomes a packet. The packet is passed to the data link layer, thus becoming a frame. This frame is then converted into bits and is passed across the network medium. This is data encapsulation. For the CCNA test, you should know the following:
Application layer -- Data
Transport layer -- Segment
Network layer -- Packet
Data link layer -- Frame
There is also the Physical Layer -- Bits

What is the difference between a routing protocol and a routed protocol?

Routing protocols determine how to route traffic to the best location of a routed protocol. Examples of routing protocols are RIP, EIGRP, OSFP, and BGP. Examples of routed protocols are IP and IPX.

What 3 devices are used to segment a LAN?

Router
Switch
Bridge

Quick Notes - CABLING TECHNOLOGY

What is a straight-through cable, and when would you use it?
A straight-through cable is the same at both ends. A straight-through cable uses pins 1, 2, 3, and 6. The send and receive wires are not crossed. You should use a straight-through cable when connecting dissimilar devices. Examples include connecting PCs to switches or hubs or a router to a switch or a hub.

What is a crossover cable, and when would you use it?
A crossover cable is a cable that has the send and receive wires crossed at one of the ends. On a Category 5 cable, the 1 and 3 wires and the 2 and 6 wires are switched on one of the cable's ends. You should use a crossover cable when connecting similar devices, such as connecting a router to a router, a switch to a switch or hub, a hub to a hub, or a PC to a PC.
Important tip -- Router (think of it as a PC) to PC via 10BaseT (NIC) uses a "crossover cable". (contradicts the rule)

How do you set up a console session to a Cisco device?
To set up a console session to a Cisco device, you connect a rollover cable to the console port on the Cisco device. You then connect the other end to your PC and configure a terminal emulation application to the following com settings: 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

What is the maximum cable length for each of the following?
10Base2
10Base510
BaseT
10BaseFL
100BaseT
The maximum cable lengths are as follows:
10Base2 (thinnet) 185 meters
10Base5 (thicknet) 500 meters
10BaseT 100 meters
10BaseFL 2000 meters (400 meters in a shared environment and 2000 meters in a point-to-point environment)
100BaseT 100 meters
What does Base stand for in 10BaseT and 100BaseT?
Base in 10BaseT and 100BaseT stands for baseband. Baseband is a network technology in which only one carrier frequency (signal) is used.

What is the difference between baseband and broadband?
Baseband is a network technology in which only one carrier frequency is used (such as Ethernet). Broadband is a network technology in which several independent channels are multiplexed into one cable (for example, a T1 line)

Quick Notes - ACCESS LISTS

Besides named access lists, what are the two types of IP access lists?
The two types of IP access lists are standard and extended.

What criteria do standard IP access lists use to filter packets?
Standard IP access lists filter packets by the source address. This results in the packet's being permitted or denied for the entire protocol suite based on the source network IP address.

What criteria do extended IP access lists use to filter packets?
Extended IP access lists filter packets by source address, destination address, protocols, and port numbers.

In what two ways can IP access lists be applied to an interface?
Access lists can be applied as inbound or outbound access lists. Inbound access lists process packets as they enter a router's interface and before they are routed. Outbound access lists process packets as they exit a router's interface and after they are routed.

How many access lists can be applied to an interface on a Cisco router?
Only one access list per protocol, per direction, per interface can be applied on a Cisco router. Multiple access lists are permitted per interface, but they must be for a different protocol.

How are access lists processed?
Access lists are processed in sequential, logical order, evaluating packets from the top down, one statement at a time. As soon as a match is made, the permit or deny option is applied, and the packet is not applied to any more access list statements. Because of this, the order of the statements within any access list is significant.

What is at the end of each access list?
At the end of each access list, an implicit deny statement denies any packet not filtered in the access list.

What are the number ranges used to define standard and extended IP access lists?
The number ranges used to define standard and extended IP access lists are as follows:
· Standard IP access lists 1 to 99 and 1300 to 1999· Extended IP access lists 100 to 199 and 2000 to 2699

When implementing access lists, what are wildcard masks?
Wildcard masks define the subset of the 32 bits in the IP address that must be matched. Wildcards are used with access lists to specify a host, network, or part

of a network. Wildcard masks work exactly the opposite of subnet masks. In subnet masks, 1 bits are matched to the network portion of the address, and 0s are wildcards that specify the host range. In wildcard masks, when 0s are present, the octet address must match. Mask bits with a binary value of 1 are wildcards. For example, if you have an IP address 172.16.0.0 with a wildcard mask of 0.0.255.255, the first two portions of the IP address must match 172.16, but the last two octets can be in the range 1 to 255.

What is the IOS command syntax used to create a standard IP access list?

Here is the command syntax to create a standard IP access list:
access-list access-list-number {permit deny} source-address [wildcard mask]access-list-number is a number from 1 to 99.
For example:
RouterA(config)#access-list 10 deny 192.168.0.0 0.0.0.255

After you create a standard or extended IP access list, how do you apply it to an interface on a Cisco router?

To apply an access list to an interface on a Cisco router, use the ip access-group interface command: ip access-group access-list-number {in out}For example:RouterA(config)#int s0RouterA(config-if)#ip access-group 10 in
Create a standard access list that permits the following networks:
192.168.200.0192.168.216.0192.168.232.0192.168.248.0
There are two ways to do this. First, you can create one access list that contains an entry for each network:
access-list 10 permit 192.168.200.0 0.0.0.255access-list 10 permit 192.168.216.0 0.0.0.255access-list 10 permit 192.168.232.0 0.0.0.255access-list 10 permit 192.168.248.0 0.0.0.255
A second way to do this is to create a single entry with wildcard masks:
access-list 10 permit 192.168.200.0 0.0.48.255
To see how this one statement denies all the networks, you must look at it in binary:
.200= 11001000.216= 11011000.232= 11101000.248= 11111000
All the bits match except the third and fourth bits. With wildcard masks, these are the bits you want to match. Therefore, your wildcard mask would be 00110000 in binary, which is 48.

What is the Cisco IOS command syntax used to create an extended access list?

Here is the Cisco IOS command syntax to create an extended access list:
access-list access-list-number {permit deny} protocol source-address source-wildcard [operator port] destination-address destination-wildcard [operator port]
protocol examples include IP, TCP, UDP, ICMP, GRE, and IGRP.
operator port can be lt (less than), gt (greater than), eq (equal to), or neg (not equal to) and a protocol port number.
Create an extended access list denying web traffic to network 192.168.10.0.
The following commands deny web traffic to network 192.168.10.0:
access-list 101 deny tcp any 192.168.10.0 0.0.0.255 eq wwwaccess-list 101 permit ip any any

What IOS command can you use to see whether an IP access list is applied to an interface?

The IOS command to see whether an IP access list is applied to an interface is show ip interface interface-type interface-number
For example:
RouterA#show ip interface s0
Serial0 is up, line protocol is up Internet address is 192.168.1.2/24 Broadcast address is 255.255.255.255 Address determined by non-volatile memory MTU is 1500 bytes Helper address is not set Directed broadcast forwarding is enabled Multicast reserved groups joined: 224.0.0.9 Outgoing access list is not set Inbound access list is 10 Proxy ARP is enabled Security level is default Split horizon is enabled ICMP redirects are always sent ICMP unreachables are always sent ICMP mask replies are never sent IP fast switching is enabled IP fast switching on the same interface is enabled IP Feature Fast switching turbo vector IP multicast fast switching is disabled IP multicast distributed fast switching is disabled IP route-cache flags are Fast Router Discovery is disabled IP output packet accounting is disabled IP access violation accounting is disabled TCP/IP header compression is disabled RTP/IP header compression is disabled Probe proxy name replies are disabled Policy routing is disabled Network address translation is disabled Web Cache Redirect is disabled BGP Policy Mapping is disabled

How can you display all access lists on a Cisco router?

To display all access lists on a Cisco router, use the show access-list command: RouterA#show access-listStandard IP access list 10 deny 192.168.0.0, wildcard bits 0.0.0.255Extended IP access list 101 permit tcp any any eq www permit udp any any eq domain permit udp any eq domain any permit icmp any any deny tcp 192.168.10.0 0.0.0.255 any eq wwwRouterA#

How do you figure out wildcard questions?

Identify the class192.68.12.0 - Class C24 bits for networks/29 tells us that we need an additional 5 bits29 - 24 = 5 bits5 bits = 128 + 64 + 32 + 16 + 8 = 248Default subnet mask for Class C network = 255.255.255.0New subnet mask for /29 network = 255.255.255.248To find the wildcard value:255.255.255.255 255.255.255.248
- ----------
0.0.0.7Same logic for Class B172.31.0.0 /1916 bits for networks/19 tells us we need an additional 3 bits19 - 16 = 3 bits3 bits = 128 + 64 + 32 = 224Default subnet mask for Class B network = 255.255.0.0New subnet mask for /19 network = 255.255.224.0To find the wildcard value:255.255.255.255255.255.224.0 ---------0.0.31.255 ´

Quick Notes - FRAME RELAY

What protocol does Frame Relay rely on for error checking?
Frame Relay does not rely on any certain protocol for error checking. Instead, it relies on upper-layer protocols to provide error checking. For example, Frame Relay relies on TCP to provide error checking in an IP network.

At what layers of the OSI model does Frame Relay operate?
Frame Relay operates at the two lower layers of the OSI model (data link and physical).

What is the difference between switched virtual circuits (SVCs) and permanent virtual circuits (PVCs)?
SVCs are virtual circuits that are dynamically established when data needs to be transferred and that are terminated when data transmission is complete. SVCs consist of four states: call setup, data transfer, idle, and call termination. PVCs are permanently established virtual circuits that operate in one of two states: idle or data transfer. When the PVC is idle, the connection between the DTE devices is still active.

What is a Data Link Connection Identifier (DLCI)?
A DLCI is a number that identifies the logical circuit between the router and the Frame Relay switch. It is the Frame Relay Layer 2 address. The Frame Relay switch maps DLCIs between each pair of routers to create a PVC. For IP devices at the end of each virtual circuit to communicate, their IP addresses need to be mapped to DLCIs. If you are running Cisco IOS 11.2 or later, mapping is done automatically using Inverse ARP. DLCIs have local significance. Think of DLCIs as the MAC address of the Frame Relay network.

What is the committed information rate (CIR)?
The CIR is the committed information rate, by the service provider, in bits per second, at which data will be transferred. The service provider sends any data in excess of this rate if its network has capacity at that time.

How does Frame Relay use Inverse ARP?
Frame Relay uses Inverse ARP as a way to dynamically map a network layer address to a DLCI. With Inverse ARP, the router can discover the network address of a device associated with a VC.

What is the Local Management Interface (LMI)?
The LMI is a signaling standard between a CPE device (a router) and the Frame Relay switch that is responsible for managing and maintaining status between the devices. It is autosensed with Cisco IOS Release 11.2 and later.

In Frame Relay, what is Forward Explicit Congestion Notification (FECN)?
The FECN is the bit in the Frame Relay header that signals to anyone receiving

the frame (switches and DTEs) that congestion is occurring in the same direction as the frame. Switches and DTEs can react by slowing the rate at which data is sent in that direction.

What is Backward Explicit Congestion Notification (BECN)?
The BECN is the bit in the Frame Relay header that signals to switches and DTEs receiving the frame that congestion is occurring in the direction opposite (backward) that of the frame. If switches and DTE devices detect that the BECN bit in the Frame Relay header is set to 1, they slow the rate at which data is sent in that direction.

In the Frame Relay header, what is the discard eligibility (DE) bit?
If congestion is detected on the Frame Relay network, the DE bit is turned on in the Frame Relay header. The DE bit is turned on for frames that are in excess of the CIR. The DE bit tells a switch which frames to discard if they must be discarded.

What is the default LMI type for Cisco routers that are configured for Frame Relay?
The default LMI for Cisco routers configured for Frame Relay is Cisco. If you are running Cisco IOS Release 11.2 or later, the Cisco router tries to autosense which LMI type the Frame Relay switch is using. If it cannot autosense the LMI type, the router uses Cisco as its LMI type. The three types of LMIs supported by Cisco routers are:
Cisco
ANSI
Q933a

When a router receives LMI information, it updates its VC status to one of three states. What are these three states?
The three states that a VC uses to update its status are as follows:
Active state The connection is active, and routers can exchange data.
Inactive state The local connection to the Frame Relay switch is working, but the remote router's connection to the Frame Relay switch is not working.
Deleted state Indicates that no LMIs are being received from the Frame Relay switch or that there is no service between the router and the Frame Relay switch.

How do you enable Frame Relay on a Cisco router?
To enable Frame Relay on a Cisco router, you must first enable the serial interface for Frame Relay encapsulation with the encapsulation frame-relay interface command:
RouterB(config)#int s 0
RouterB(config-if)#ip address 192.168.1.1 255.255.255.0
RouterB(config-if)#encapsulation frame-relay

The default encapsulation for a serial interface configured for Frame Relay is cisco. If you are connecting to a non-Cisco router, how do you change the

encapsulation type?
If you are connecting to a non-Cisco router in a Frame Relay network, you need to specify ietf as the encapsulation type:
RouterB(config-if)#ip address 192.168.1.1 255.255.255.0
RouterB(config-if)#encapsulation frame-relay ietf

If you are using Cisco IOS Release 11.1 or earlier, or if you do not want to autosense the LMI type, how do you define the LMI type on a Cisco router?
To define the LMI type on a Cisco router, use the frame-relay lmi-type {ansi cisco q933a} interface command:
RouterB(config-if)#ip address 192.168.1.1 255.255.255.0
RouterB(config-if)#encapsulation frame-relay
RouterB(config-if)#frame-relay lmi-type ansi

If Inverse ARP is disabled on your router, how do you reenable it?
Inverse ARP is enabled by default on a Cisco router. If it is disabled, reenable it by using the following command:
RouterB(config-if)#frame-relay inverse-arp [protocol] [dlci]
Supported protocols indicated by the protocol option include ip, ipx, decnet, appletalk, vines, and xns.
If a remote router does not support Inverse ARP, you must define the address-to-DLCI table
statically. How do you create these static maps?
To define static maps on a Cisco router, use the following command:
RouterA(config-if)#frame-relay map protocol protocol-address dlci [broadcast] [ietf cisco] [payload-compress packet-by-packet]
where: · protocol defines the supported protocol bridging or LLC.
· protocol-address is the remote router's network layer address.
· dlci defines the remote router's local DLCI.
· broadcast specifies whether you want to forward broadcasts over the VC, permitting dynamic routing protocols over the VC.· ietf cisco is the encapsulation type.
How do you display the encapsulation type, DLCI, LMI type, and whether the device is a DTE or DCE on a serial interface?
To display the interface's encapsulation type, DLCI number, LMI type, and whether the device is a DTE or DCE, use the show interface interface-type interface-number command: RouterA#show int s0
Serial0 is up, line protocol is up Hardware is HD64570 Internet address is 192.168.1.2/24 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255 Encapsulation FRAME-RELAY, loopback not set, keepalive set (10 sec) LMI enq sent 3, LMI stat recvd 0, LMI upd recvd 0, DTE LMI up LMI enq recvd 5, LMI stat sent 0, LMI upd sent 0 LMI DLCI 1023 LMI type is CISCO frame relay DTE Broadcast queue 0/64, broadcasts sent/dropped 0/0, interface broadcasts 0 Last input 00:00:05, output 00:00:07, output hang never Last clearing of "show interface" counters never Input queue: 0/75/0 (size/max/drops); Total output drops: 0 Queueing strategy: weighted fair

What Cisco IOS command displays the LMI traffic statistics and LMI type?

The show frame-relay lmi command displays the LMI traffic statistics and LMI type: RouterA#show frame-relay lmi

LMI Statistics for interface Serial0 (Frame Relay DTE)
LMI TYPE = CISCO Invalid Unnumbered info 0
Invalid Prot Disc 0 Invalid dummy Call Ref 0
Invalid Msg Type 0 Invalid Status Message 0
Invalid Lock Shift 0 Invalid Information ID 0
Invalid Report IE Len 0 Invalid Report Request 0
Invalid Keep IE Len 0 Num Status Enq. Rcvd 1748
Num Status msgs Sent 1748 Num Update Status Sent 0
Num St Enq. Timeouts 0
routera#

How do you display the current Frame Relay map entries and information about these connections on a Cisco router?

To view the current map entries and information about the connections, use the show frame-relay map command:

RouterA#show frame-relay map
Serial0 (up): ip 192.168.1.2 dlci 100(0x64,0x1840), dynamic,
Broadcast, status defined, active

How do you clear dynamic Frame Relay maps that were created by Inverse ARP?

Use the clear frame-relay-inarp privileged EXEC command to clear dynamic Frame Relay maps created by Inverse ARP.

Quick Notes - ROUTING

How do OSPF-enabled routers build adjacencies and exchange their routing tables?
OSPF-enabled routers build adjacencies by sending Hello packets out through all OSPF-enabled interfaces.

If these routers share a command link and agree on parameters set within their Hello packets then they become neighbors. If these parameters differ then the routers do not become neighbors and communication stops.

OSPF routers form adjacencies with certain routers. These routers are determined by the layer 2 (data link) media type and as soon as the adjacencies are formed each router sends LSAs (Link State Advertisements) to all adjacent routers. The LSAs describe the state of each router's links. There are multiple LSA types and a route that receives an LSA from a neighbor records the LSA in a link-state database and floods a copy of the LSA to all its other neighbors.

When all databases are complete - then each router uses the SPF (Shortest-Path First) algorithm to calculate a loop-free topology and builds its routing table based on this topology.
It is important to note that the Hello protocol is bidirectional and is the means by which neighbors are discovered and acts as keepalives between neighboring routers. It also establishes and maintain neighbor relationships and elects the DR (Designated Router) and BDR (Backup Designated Router) to represent the segment on Broadcast and NBMA (nobroadcast multiaccess) networks.

Note: Hello protocols are sent periodically sent out each OSPF-enabled interface using IP multicast address 224.0.0.5. The default interval on NBMA (nonbroadcast multiaccess) networks is 30 seconds. The default interval on Broadcast, Point-to-point, and point-to-multipoint networks is 10 seconds.

What are LSAs (link-state advertisements)?
LSAs are sent out all OSPF-enabled router interfaces describing the state of the router's links. They are also packets that OSPF uses to advertise changes in the condition of a link or other OSPF routers.

Name two LSA (link-state advertisement) types?
Type 1 LSAs are router LSAs and are generated by each router for the area to which the router belongs. These LSAs describe the states of the router'links to the area (area 0 for example) and are flooded within a single area (area 0 for example).
Type 2 LSAs are network LSAs and are generated by the DR (Designated Router) and the BDR (Backup Designated Router). They describe the routers attached to a particular network and are flooded within a single area (area 0 for example).

What is the routing metric OSPF is based on?
Bandwith.
Formula: Cost = 100,000,000 / bandwidth in bits per seconds
The cost of a 100 MBbps connection would be:
1000,000,000 / 100,000,000 =1

Based on the schema above -- if adjacencies are established with only with the DR (Designated Router) and BDR (Backup Designated Router)- what is the circuit count?
Formula:
2(n - 1) where n is the number of routers in the network.
2(5 - 1) = 8 circuits.
A circuit can also be thought of as an adjacency or connection.
Count four going into the DR and 4 going into the BDR for a total of 8.

Note: OSPF avoids synchronizing between every pair of routers in the network by using a DR and BDR. This way adjacencies are formed only to the DR and BDR, and the number of LSAs sent over the network is reduced. Now only the DR and BDR have four adjacencies, and all the other routers have two.

On an OSPF-enabled router -- what is the router ID and where does an OSPF-enabled router receive its router ID?
To initialize - OSPF must be able to define a router ID. The most common and stable source for a router ID is the IP address set on the logical loopback interface that is always available. If no logical interface is defined -- then the router receives its ID from the highest IP address on the physical interfaces.

Note: If two loopback addresses are defined -- it will use the highest loopback address. Think highest logical or highest physical interface address.

Name five OSPF network types:
Broadcast networks: Ethernet/Token Ring. OSPF-enabled routers on broadcast networks elect a DR (Designated Router) and BDR (Backup Designated Router). All the routers in the network form adjacencies with the DR and BDR. Note: OSPF packets are multicast to the DR and BDR.

NBMA (nonbroadcast multiaccess) networks: Frame Relay/X.25/ATM. NBMA networks can connect more than two routers but have no broadcast functionality. These networks elect an DR and BDR. Note: OSPF packets are unicast.

Point-to-point networks: A physical DS1 (T1) for example.
Point-to-point networks connect a pair of routers and always becomes adjacent.
Point-to-multipoint networks: Point-to-multipoint networks are a special configuration of NBMA networks in which networks are treated as a collection of point-to-point links. Point-to-multipoint networks do not elect a DR or BDR. Note:

OSPF packets are multicast.

Virtual links: Virtual links area special configuration that the router interprets as unnumbered point-to-point networks. The network administrator creates/defines virtual links.

What is routing?
Routing is the process in which items are forwarded from one location to another. Routing is a hop-by-hop paradigm.
A Cisco router performs routing and switching functions. Describe what each function does.
Routing is a way to learn and maintain awareness of the network topology. Each router maintains a routing table in which it looks up the destination Layer 3 address to get the packet one step closer to its destination.The switching function is the actual movement of temporary traffic through the router, from an inbound interface to an outbound interface.

What are the three types of routes you can use in a Cisco router?
The three types of routes are static routes, dynamic routes, and default routes.

What is the difference between static and dynamic routes?
Static routes are routes that an administrator manually enters into a router. Dynamic routes are routes that a router learns automatically through a routing protocol.

How do you configure a static route on a Cisco router?
To configure a static route on a Cisco router, enter the ip route destination-network [mask] {next-hop-address outbound-interface} [distance] [permanent] global command. Here's an example:
RouterB(config)#ip route 172.17.0.0 255.255.0.0 172.16.0.1

This example instructs the router to route to 172.16.0.1 any packets that have a destination of 172.17.0.0 to 172.17.255.255

What is a default route?
Also known as the gateway of last resort, a default route is a special type of static route with an all-zeros network and network mask. The default route is used to route any packets to a network that a router does not directly know about to a next-hop router. By default, if a router receives a packet to a destination network that is not in its routing table, it drops the packet. When a default route is specified, the router does not drop the packet. Instead, it forwards the packet to the IP address specified in the default route.

How do you configure the default route on a Cisco router?
To configure a default route on a Cisco router, enter the following global configuration command:
ip route 0.0.0.0 0.0.0.0 [ip-address of the next-hop router outbound-interface]

For example:
RouterB(config)#ip route 0.0.0.0 0.0.0.0 172.16.0.2

What is a routing protocol?
A routing protocol defines the set of rules used by a router when it communicates with neighboring routers. Routing protocols listens for packets from other participants in order to learn and maintain a routing table.

What are the two major types of routing protocols?
The two major types of routing protocols are
· Interior Gateway Protocol (IGP)
· Exterior Gateway Protocol (EGP)
IGP is used to exchange routing information among routers in the same autonomous system (AS). EGP is used to communicate between ASs.

Note: For more information about autonomous systems, see Interconnecting Cisco Network Device (Cisco Press).

What is administrative distance?
Administrative distance (AD) is an integer from 0 to 255 that rates the trustworthiness of routing information received on a router from a neighboring router. The AD is used as the tiebreaker when a router has multiple paths from different routing protocols to the same destination. The path with the lower AD is the one given priority.

What are the three classes of routing protocols?
The three classes of routing protocols are
· Distance vector· Link-state· Balanced hybrid

What is the AD for each of the following?
· Directly connected interface
· Static route
· EIGRP
· IGRP
· OSPF
· RIP
· External EIGRP
· Unknown
The ADs are as follows:
Directly connected interface 0
Static route 1
EIGRP 90
IGRP 100
OSPF 110
RIP 120
External EIGRP 170

Unknown 255

How do distance vector routing protocols function?
Also known as Bellman-Ford-Fulkerson algorithms, distance vector routing protocols pass complete routing tables to neighboring routers. Neighboring routers then combine the received routing table with their own routing table. Each router receives a routing table from its directly connected neighbor. Distance vector routing tables include information about the total cost and the logical address of the first router on the path to each network they know about.

How do distance vector routing protocols keep track of any changes to the internetwork?
Distance vector routing protocols keep track of an internetwork by periodically broadcasting updates out all active interfaces. This broadcast contains the entire routing table. This method is often called routing by rumor.
Slow convergence of distance vector routing protocols can cause inconsistent routing tables and routing loops.

What are some mechanisms that distance vector protocols implement to prevent routing loops and inconsistent routing tables?
Here are some of the ways distance vector routing protocols prevent routing loops and inconsistent routing tables:
· Maximum hop count· Split horizon
· Route poisoning· Holddowns

What is maximum hop count?
If a loop is in an internetwork, a packet loops around the internetwork forever. Maximum hop counts prevent routing loops by defining the maximum number of times a packet will loop around the internetwork. RIP uses a hop count of up to 15, so anything that requires 16 hops is unreachable. Anytime a packet passes through a router, it is considered one hop.

What is split horizon?
The rule of split horizon is that it is never useful to send information about a route back in the direction from which the original update came.

What is convergence?
Convergence is when all routers have consistent knowledge and correct routing tables.

What is route poisoning?
With route poisoning, when a distance vector routing protocol notices that a route is no longer valid, the route is advertised with an infinite metric, signifying that the route is bad. In RIP, a metric of 16 is used to signify infinity. Route poisoning is used with holddowns.

What are hold-down timers?
Hold-down timers prevent regular update messages from reinstating a route that might have gone bad. Hold-down timers also tell routers to hold for a period of time any changes that might affect routes.

What are triggered updates?
When a router notices that a directly connected subnet has changed state, it immediately sends another routing update out its other interfaces rather than waiting for the routing update timer to expire. Triggered updates are also known as Flash updates.

What is IP RIP?
IP RIP is a true distance vector routing protocol that sends its complete routing table out all active interfaces every 30 seconds. IP RIP uses a hop count as its metric to determine the best path to a remote network. The maximum allowable hop count is 15, meaning that 16 is unreachable. There are two versions of RIP. Version 1 is classful, and version 2 is classless. IP RIP can load-balance over as many as six equal-cost paths.

What four timers does IP RIP use to regulate its performance?
Here are the four timers that IP RIP uses to regulate its performance: · Route update timer Time between router updates. The default is 30 seconds.· Route invalid timer Time that must expire before a route becomes invalid. The default is 180 seconds.· Route hold-down timer If IP RIP receives an update with a hop count higher than the metric recorded in the routing table, the router goes into holddown for 180 seconds.· Route flush timer Time from when a route becomes invalid to when it is removed from the routing table. The default is 240 seconds.

How do you enable RIP on a Cisco router?
To enable RIP on a Cisco router, start by using the router global configuration command, followed by the rip protocol. This selects RIP as the routing protocol. Then you assign the network command, followed by the directly connected network number(s) you want to activate RIP on. Here's an example:
RouterB(config)#router rip

RouterB(config-router)#network 192.168.1.0
RouterB(config-router)#network 192.168.2.0

How do you stop RIP updates from propagating out an interface on a router?
Sometimes you do not want RIP updates to propagate across the WAN, wasting valuable bandwidth or giving out valuable information about your internetwork. The easiest way to stop RIP updates from propagating out an interface is to use the passive-interface global configuration command.

How do you display the contents of a Cisco IP routing table?

The show ip route command displays the Cisco routing table's contents.

What is Interior Gateway Routing Protocol (IGRP)?
IGRP is a Cisco proprietary distance vector routing protocol. IGRP has a default hop count of 100 hops, with a maximum hop count of 255. IGRP uses bandwidth and line delay as its default metric, but it can also use reliability, load, and MTU.

How do you enable IGRP on a Cisco router?
The way you enable IGRP on a Cisco router is similar to the way you enable RIP, except you specify IGRP as the protocol and add an autonomous system number. For example:
RouterA(config)#router igrp 10 (10 is the AS number)
RouterA(config-router)#network 192.168.0.0
RouterA(config-router)#network 192.168.1.0
RouterA(config-router)#network 192.168.2.0

What four timers does IGRP use to regulate its performance?
The four timers IGRP uses to regulate its performance are as follows:

· Route update timer Time between router updates The default is 90 seconds.

· Route invalid timer Time that must expire before a route becomes invalid . The default is 270 seconds.

· Route hold-down timer If a destination becomes unreachable, or if the next-hop router increases the metric recording in the routing table, the router goes into holddown for 280 seconds.

· Route flush timer[md]Time from when a route becomes invalid to when it is removed from the routing table. The default is 630 seconds

Quick Notes - SWITCHING

What are three types of LAN traffic?
Unicasts - intended for one host.
Broadcasts - intended for everyone.
Multicasts - intended for a only a subset or group within an entire network.

What are unicast frames?
Unicast frames are the most common type of network traffic. A unicast frame is a frame intended for only one host. The only station that processes this frame is one station that has its own MAC address in the destination portion of packet.

What are broadcast frames?
Broadcast frames are frames intended for everyone. Stations view broadcast frames as public service announcements. All stations receive and process broadcast frames. In large networks, broadcasts can cause serious performance degradation in network hosts - (broadcast storm).
The destination address of broadcast frames (Data Link / Layer 2 broadcast addresses is FF-FF-FF-FF-FF-FF or alternatively all 1s in binary (11111111).

What are multicast frames?
Multicast frames address a group of devices that have a common interest. These frames allow the source to send only one copy of the frame on the network even though it is intended for several stations. Only stations that have a card that is configured by software to receive multicast frames for a particular multicast group can process a frame to that multicast address - all other stations discard multicast frames. An example of a multicast frame is: 01:00:5E:01:01:01/ The "01" at the beginning of the address signifies that it is an Ethernet multicast frame.

What three major functions do Data Link Layer / Layer 2 Switches perform?
Address learning
Packet forwarding/filtering
Loop avoidance by spanning tree

What will occur when you attempt to segment a network with hubs and repeaters?
Basically, hubs and repeaters become extensions of the physical cable plant. All devices that connect to either a hub or a repeater share the same bandwidth and by definition hubs and repeaters create a single broadcast and collision domain. Think of both devices are pass-through devices much like a electrical power-strip. Hubs and repeaters reside on the Physical Layer / Layer 1 of the OSI model where they pass 0s and 1s along the wire or up to the Data Link Layer. CSUs / Channel Service Units fall into the same category. All are regarded as unintelligent devices. No addressing takes place on the Physical layer.

What is the advantage of segmenting a network with bridges or switches?

Bridges and switches function on the Data Link Layer / Layer 2 of the OSI model and filter by MAC address. Each port on either device provides full, dedicated bandwidth and creates a single collision domain.
Very important:
Because bridges and switches operate a Layer 2 -- they cannot filter broadcasts, and they create a single broadcast domain. (Note: each nailed-up port on a switch is a single Collision Domain - there will be a schematic on the exam to test your knowledge on broadcast and collision domains.)
Also, bridges are implemented by software and normally have a couple of network ports; whereas switches are implemented in hardware by ASIC chips and have many ports.
Think Data Link Layer / Layer 2 of the OSI model - physical addresses / MAC addresses
List some advantages Layer 2 switches have over bridges:
· High-speed backplane - multiple simultaneous conversations.
· Data-buffering capabilities are used to store-and-forward packets to the correct port(s).
· Lower latency than bridges. Remember that switches are implemented in hardware not software. Much faster.
· Higher port count or density.

What are the pros can cons of segmenting a LAN with routers?

Pros: Each interface on a router creates a single broadcast and collision domain. Routers function or operate on the Network Layer / Layer 3 of the OSI model and do not propagate broadcasts*. (* very important concept)

Cons: Routers are not transparent and are implemented in software thereby introducing latency in the network.

Remember: Routers = Network Layer / Layer 3 on the OSI model - Logical addressing (IP address).

Functions: Two key functions: routing and switching. The routing component is responsibile for learning and maintaining awareness of the network topology. The switching function is the process of moving packets from an inbound interface (Ethernet 0 for example) to an outbound interface (Serial 0 for example). Path selection is a key term.

What three devices are used to segment a LAN?
Router - logical addressing - IP address
Switch - physical addressing - MAC address
Bridge - physical addressing - MAC addres

What is microsegmentation?
Each workstation or network device on the network has its own dedicated segment - also known as a Collision Domain - to a switch. Each device gets the

segments full bandwidth and does not have to share the dedicated segment with other devices. Collisions are reduced because each segment is its own Collision Domain.

Important: Full-duplex transmission is achieved by microsegmentation. Each device can send and receive at the same time which doubles the amount of bandwidth between nodes.

What are the three switching methods in Cisco Catalyst switches?
The three frame operating modes to handle frame switching are
Store-and-forward
Cut-through
Fragment-free

What is the Cisco Catalyst store-and-forward switching method?
In the store-and-forward switching method, the switch receives the entire frame before it forwards it. The switch reads the cyclic redundancy check (CRC) to make sure the frame is not bad. If the frame is good, the switch forwards it. Because the switch stores the frame before forwarding it, latency is introduced in the switch. Latency through the switch varies with the size of the frame.

What is the Cisco Catalyst cut-through switching method?
In cut-through switching mode, the switch only checks the frame's destination address and immediately begins forwarding the frame out the appropriate port. Because the switch checks the destination address in only the header and not the entire frame, the switch forwards a collision frame or a frame that has a bad CRC.

What is the Cisco Catalyst fragment-free switching method?
Also known as modified cut-through, fragment-free switching checks the first 64 bytes before forwarding the frame. Ethernet specifications state that collisions should be detected during the first 64 bytes of the frame. By reading the first 64 bytes of the frame, the switch can filter most collisions, although late collisions are still possible.

What is the default switching mode in Cisco Catalyst 1900 switches?
The default switching mode for the Catalyst 1900 is fragment-free.

What is half-duplex transmission mode?
Half-duplex transmission is the default mode that Ethernet functions in. In half-duplex transmission, a device can only send or receive--not do both at once. In half-duplex mode, stations are susceptible to collisions, and efficiency is rated at 50 to 60 percent.

What is full-duplex transmission mode?
In full-duplex mode, a station can send and receive at the same time. In full-duplex mode, collision detection is disabled. This mode offers 100 percent efficiency in both directions.

On a Cisco Catalyst 1900 switch, what are the default duplex settings for 10BaseT/100BaseT ports, default switching mode, and default protocols?
The factory default settings for a Catalyst 1900 switch are as follows: · IP address: 0.0.0.0· CDP enabled· Switching mode: fragment-free· 10BaseT ports: half-duplex· 100BaseT ports: autonegotiate· Spanning tree enabled· No console password

What are the two configuration modes in a Catalyst 1900 switch?
Configuring a Catalyst 1900 switch is similar to configuring a router. The two configuration modes available are global configuration mode and interface configuration mode

How do you configure an IP address and subnet mask on a Catalyst 1900 switch?
To configure an IP address and subnet mask on a Catalyst 1900 switch, use the ip address address mask global configuration command:
Cat1900(config)#ip address 192.168.0.2 255.255.255.0

Why would you want to assign an IP address to a Layer 2 device, such as a switch?
You would assign an IP address to a Layer 2 device for management and configuration. With an IP address enabled on a Cisco switch, you can Telnet into it and change the configuration. You can also enable SNMP on the device and remotely monitor the switch.

How do you configure a default gateway on a Cisco Catalyst 1900 switch?
To configure a default gateway on a Catalyst 1900 switch, use the ip default-gateway ip address global configuration command. The following example configures the switch to use IP address 192.168.0.1 as its default gateway:
Cat1900(config)#ip default-gateway 192.168.0.1
To remove the default gateway, use the no ip default-gateway command.

On a Catalyst 1900 switch, what command can you use to view the switch's IP address, subnet mask, and default gateway?
The show ip command displays the switch's IP address, subnet mask, and default gateway. Here's an example:
Cat1900#show ipIP Address: 192.168.0.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.0.1
Management VLAN: 1
Domain name:
Name server 1: 0.0.0.0
Name server 2: 0.0.0.0
HTTP server : Enabled
HTTP port : 80
RIP : Enabled
Cat1900#

How do you change the duplex mode on a Catalyst 1900 switch?
To change the duplex mode on a Catalyst 1900 switch, use this command:
duplex {auto full full-flow-control half}
The following example changes the duplex speed for Ethernet interface 1 on the switch to full duplex:

Cat1900(config)#interface e0/1
Cat1900(config-if)#duplex full

How do you change the duplex mode on a Catalyst 1900 switch?
To change the duplex mode on a Catalyst 1900 switch, use this command:
duplex {auto full full-flow-control half}
The following example changes the duplex speed for Ethernet interface 1 on the switch to full duplex:
Cat1900(config)#interface e0/1
Cat1900(config-if)#duplex full

What command can you use to view the duplex settings and spanning tree state of a Catalyst switch?
You use the show interface type module/port EXEC command to view the duplex settings and spanning tree state. This example shows the output for the show interface command on Ethernet interface 0/1:
Cat1900#show interface e0/1
Ethernet 0/1 is Suspended-no-link
beatHardware is Built-in 10Base-TAddress is 0010.F621.F681MTU 1500 bytes, BW 10000 Kbits802.1d

STP State: Forwarding
Forward Transitions: 1
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description:Duplex setting: Full duplex
Back pressure: Disabled

What command can you use to check for frame check sequence (FCS) or late collision errors?
The show interface type module/port EXEC command displays FCS or late collision errors. Cat1900#show interface e0/1
Receive Statistics Transmit Statistics
---------- ----------
Total good frames 0 Total frames 0Total octets 0 Total octets 0 Broadcast/multicast frames 0 Broadcast/multicast frames 0Broadcast/multicast octets 0 Broadcast/multicast octets 0Good frames forwarded 0 Deferrals 0Frames filtered 0 Single collisions 0 Runt frames 0 Multiple collisions 0No buffer discards 0 Excessive collisions 0 Queue full discards 0Errors: Errors: FCS

errors 0 Late collisions 0 Alignment errors 0 Excessive deferrals 0 Giant frames 0 Jabber errors 0 Address violations 0 Other transmit errors 0

How do you display the MAC address table on a Catalyst 1900 switch?
The show mac-address-table EXEC command displays the MAC address table and also tells you whether the MAC address entry is dynamic, permanent, or static. Here's an example: Cat1900#show mac-address-table
Address Dest Interface Type Source Interface List

0080.C6E7.9CEF Ethernet 0/21 Dynamic All0030.80EF.988C Ethernet 0/22 Dynamic All
0040.05A2.5E92 Ethernet 0/11 Dynamic All

What are dynamic addresses on a Catalyst switch?
Dynamic addresses are addresses that the switch learns about dynamically through the learning process. If the switch does not see a MAC address for a certain amount of time, it drops the MAC address.

What are permanent MAC addresses on a Catalyst switch?
Permanent MAC addresses are entered manually by the administrator and are not aged out.

On a Catalyst 1900 switch, how do you make a MAC address permanent?
To make a MAC address permanent, use the mac-address-table permanent mac-address type module/port global command. The following example makes MAC address 0080.C6E7.9CEF permanent in the CAM table for port 0/21:

Cat1900(config)#mac-address-table permanent 0080.C6E7.9CEF Ethernet 0/21

What is the maximum number of MAC addresses a Catalyst 1900 can store in its MAC address table?
The maximum number of MAC addresses a Catalyst 1900 can store in its MAC address table is 1024.

What are static MAC addresses in a Catalyst 1900 switch?
On a Catalyst 1900 switch, static addresses allow you to restrict a MAC address to a specific port.

How do you restrict a MAC address to a specific port on a Catalyst 1900 switch?
To restrict a MAC address to a specific port, use the mac-address-table restricted static mac-address type module/port src-if-list global command:
Cat1900(config)#mac-address-table restricted static aaaa.aaaa.aaaa e0/1
This restricts MAC address aaaa.aaaa.aaaa to Ethernet port 0/1.

What EXEC command can you use to show the port security configurations on a Catalyst 1900 switch?
The show mac-address-table security command displays the port security

configurations: Cat1900#show mac-address-table security
Action upon address violation : Suspend Interface Addressing Security Address Table Size Clear Address
---
Ethernet 0/1 Disabled N/A NoEthernet 0/2 Disabled N/A NoEthernet 0/3 Enabled 100 NoEthernet 0/4 Disabled N/A NoEthernet 0/5 Disabled N/A NoEthernet 0/6 Disabled N/A NoEthernet 0/7 Disabled N/A NoEthernet 0/8 Disabled N/A NoEthernet 0/9 Disabled N/A No

What Catalyst command can you use to display information about the IOS software version and hardware information about the switch?
The show version EXEC command displays the IOS software version and hardware information about the switch. The following example shows the output of the show version command on a Catalyst switch:
Cat1900#show version
Cisco Catalyst 1900/2820 Enterprise Edition SoftwareVersion V9.00.04 written from 192.168.000.001Copyright (c) Cisco Systems, Inc. 1993-1999Cat1900 uptime is 0day(s) 01hour(s) 34minute(s) 47second(s)cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memoryHardware board revision is 1Upgrade Status: No upgrade currently in progress.Config File Status: No configuration upload/download is in progress27 Fixed Ethernet/IEEE 802.3 interface(s)Base Ethernet Address: 00-10-F6-21-F6-80
show version will show up on the exam for sure - router or switch.

What Catalyst command do you use to back up the running configuration to a TFTP server?
Use the copy nvram tftp://host/dst_file command to back up the running configuration to a TFTP server:
Cat1900#copy nvram tftp://192.168.0.3/cat1900.cfg
Configuration upload is successfully completed
Cat1900#

How do you restore a configuration file from a TFTP server on a Catalyst 1900 switch?
To restore a configuration file from a TFTP server, use the copy tftp://host/src_file nvram command:
Cat1900#copy tftp://192.168.0.3/cat1900.cfg nvram
TFTP successfully downloaded configuration file
Cat1900#

What Catalyst 1900 command would you use to restore the switch to its factory settings?
To restore a 1900 series switch to its factory settings, use the delete nvram command.

Note: For some reason I think this one was on my exam.

Quick Notes - Network Management

What is the Cisco Discovery Protocol (CDP)?
CDP is a Cisco proprietary protocol that runs on all Cisco IOS-enabled devices. It is used to gather information about directly connected neighboring devices. CDP operates at Layer 2 of the OSI model and is media-independent. With CDP, you can tell the hardware type, device identifier, address list, software version, and active interfaces on neighboring Cisco devices. CDP is enabled by default on all Cisco equipment. It uses a nonroutable SNAP frame to communicate between devices.

Note: Because CDP is media-independent it can operate over most media types. The only media types CDP cannot operate over are X.25, because it doesn't support SNAP encapsulation, and Frame Relay point-to-multipoint interfaces.

What are three reasons to disable CDP?
Three reasons to disable CDP are as follows:
. To save network bandwidth by not exchanging CDP frames.
. If you are connecting to non-Cisco devices.
. Security. CDP broadcasts information about the device every 60 seconds. Sniffers and other devices can view these broadcasts to discover information about your network.

How do you disable CDP on Cisco routers?
Two commands disable CDP on a Cisco router. To disable CDP on the entire device, use the no cdp run global command:
RouterB(config)#no cdp run
To disable CDP on an interface only, use the no cdp enable interface command:
RouterB(config)#int e0
RouterB(config-if)#no cdp enable
This disables CDP on Ethernet interface 0.

What does the show CDP command display?
The show CDP command displays global CDP information about the device. It tells you when the device will send CDP packets and the CDP holdtime:
RouterB#show cdp
Global CDP information:

Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds

Note: For the CCNA test, remember that the default time a device will send out CDP information is 60 seconds and the default holdtime is 180 seconds.

On a Cisco router, what does the show cdp neighbors command display?
The show cdp neighbors command displays the following:

· Device ID (name of the device)
· The local interface (local outgoing port)
· The holdtime displayed in seconds
· The device's capability code (this tells you if the device is a router, switch, or repeater)
· Hardware platform of the neighboring device (what type of Cisco device it is and the model)
· Port ID of the neighboring device (remote port)
RouterB#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater
Device ID Local Intrfce Holdtme Capability Platform Port ID
RouterA Ser 0 146 R 2505 Ser 0

What does the show cdp neighbors detail command display?
The show cdp neighbors detail and show cdp entry * commands show the same output. They both display the following:
· Device ID (host name) of the remote neighbor
· Layer 3 address of the remote device (if the device has more than one Layer 3 address on its interface, only the primary address is shown)
· Device platform and capabilities· Local interface and outgoing port ID
· Remote device holdtime in seconds
· IOS type and version
RouterB#show cdp neighbors detail

Device ID: RouterA
Entry address(es):
IP address: 192.168.2.1
Platform: cisco 2505, Capabilities: Router
Interface: Serial1, Port ID (outgoing port): Serial1
Holdtime : 164 sec Version :Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-D-L), Version 12.0(13), RELEASE SOFTWARE (fc1)Copyright (c) 1986-2000 by cisco Systems, Inc.Compiled Wed 06-Sep-00 01:08 by Linda

What does the show cdp traffic command display?
The show cdp traffic command displays information about interface traffic. This includes the number of CDP packets sent and received and CDP errors:
RouterB#show cdp traffic
CDP counters :
Packets output: 105, Input: 103
Hdr syntax: 0, Chksum error: 0, Encaps failed:
No memory: 0, Invalid packet: 0, Fragmented: 0

What does the show cdp interface command display?

The show cdp interface command displays the status of CDP on all interfaces on your device: RouterB#show cdp interface
Ethernet0 is up, line protocol is down
Encapsulation ARPA
Sending CDP packets every 60 seconds Holdtime is 180 seconds
Serial0 is up, line protocol is up
Encapsulation HDLC
Sending CDP packets every 60 seconds Holdtime is 180 seconds
Serial1 is up, line protocol is up
Encapsulation HDLC
Sending CDP packets every 60 seconds Holdtime is 180 seconds

What Cisco IOS router command can you use to see a neighbor router's IP address?
To see a neighbor router's IP address, you must use the show cdp neighbor detail or show cdp entry * user mode or EXEC command. (This one will probably be on the exam)

What IOS command do you use to view the active outbound telnet sessions for the current user on a Cisco router?
The show sessions command displays the active outbound telnet sessions from that particular user on your router.
RouterA#show sessions
Conn Host Address Byte Idle Conn Name
* 1 192.168.1.2 192.168.1.2 0 0 192.168.1.2

What key sequence do you use to suspend a Telnet session on a remote system and return to your local router?
To suspend a Telnet session, press Ctrl-Shift-6, and then press X.

How do you end a remote Telnet session on a Cisco router?
To end a Telnet session, use the exit or logout command while you're on the remote device: RouterB>exit
[Connection to 192.168.1.2 closed by foreign host]
RouterA#
Upon using the ping EXEC command, you receive one of the following responses:
· .
· !
· ?
· C
· U
· I
What does each of these responses mean?
. = Each period indicates that the network server timed out while waiting for a reply.

! =Each exclamation point indicates the receipt of a reply.
? =Unknown packet type.
C =A congestion experienced packet was received.
U =A destination unreachable error PDU was received.
I = The user interrupted the test.

What is the trace EXEC command used for?
RouterA#trace 192.168.2.2
Type escape sequence to abort.
Tracing the route to 192.168.2.2
1 192.168.2.2 16 msec 16 msec *
Note: If trace responds with a * it means the probe timed out. If it responds with a ? it means it received an unknown packet type.

What are the two ways in which a Cisco router resolves host names to IP addresses?
A Cisco router resolves host names using either a host table on each router or a DNS server.

What is the main purpose of RAM on a Cisco router?
On most Cisco routers, the IOS is loaded into RAM, as well as the running configuration. It is also used to hold routing tables and packet buffers.

What is the function of ROM on a Cisco router?
On a Cisco router, ROM is used to start and maintain the router.

What is Flash memory used for on a Cisco router?
Flash memory is used to store the Cisco IOS software image and, if there is room, multiple configuration files or multiple IOS files. On some routers (the 2500 series), it is also used to run the IOS.

What is the function of NVRAM on a Cisco router?
Nonvolatile Random-Access Memory (NVRAM) is used to hold the saved router configuration. This configuration is not lost when the router is turned off or reloaded.

What is the main purpose of the configuration register on a Cisco router?
The configuration register's main purpose is to control how the router boots up. It is a 16-bit software register that by default is set to load the Cisco IOS from Flash memory and to look for and load the startup-config file from NVRAM.
What Cisco IOS command would you use to view the current configuration register value?
The show version command is used to display the router's current configuration register: RouterA#show version
Cisco Internetwork Operating System SoftwareIOS (tm) 2500 Software (C2500-D-L),

Version 12.0(13), RELEASE SOFTWARE (fc1)Copyright (c) 1986-2000 by cisco Systems, Inc.Compiled Wed 06-Sep-00 01:08 by lindaImage text-base: 0x030388F8, data-base: 0x00001000 Configuration register is 0x2102

How do you change the configuration register on a Cisco router?
To change the configuration register on a Cisco router, use the config-register global command.

What Cisco IOS command displays the contents of Flash memory?
The show flash command displays the contents of Flash memory. This includes the images stored in Flash memory, the images' names, bytes used in Flash memory, bytes available, and the total amount of Flash memory on your router:
RouterA#show flash
System flash directory:File Length Name/status
1 6897716 c2500-d-l.120-13.bin[6897780 bytes used, 1490828 available, 8388608 total]8192K bytes of processor board System flash (Read ONLY)

What IOS command would you use to copy the running configuration on a router to a TFTP server?
To copy the running configuration to a TFTP server, use the copy running-config tftp privileged EXEC command:
RouterB#copy run tftp
Address or name of remote host []? 192.168.0.2
Destination filename [routerb-confg]?
!!
780 bytes copied in 6.900 secs (130 bytes/sec)
This gives you a backup of your running config on a TFTP server.

How do you erase the router's configuration and bring it back to the factory default?
The erase startup-config privileged EXEC command erases your router's configuration, thus bringing it back to its factory defaults:

RouterB#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]Erase of nvram: complete
Note: In order to complete the process, you need to reload the router. An older IOS command that you can use to accomplish the same results is write erase.

How do you restore a configuration file from a TFTP server into your Cisco router's RAM?
The copy tftp running-config privileged EXEC command merges the saved and running configuration into your router's RAM, so any commands not explicitly change or removed will remain in the running configuration.
RouterB#copy tftp running-config

Address or name of remote host []? 192.168.0.2
Source filename []? routerb-confg
Destination filename [running-config]?
Accessing tftp://192.168.0.2/routerb-confg...
Loading routerb-confg from 192.168.0.2 (via Ethernet0):
!
[OK - 780/1024 bytes] 780 bytes copied in 4.12 secs (195 bytes/sec)
RouterB# 01:40:46: %SYS-5-CONFIG: Configured from
tftp://192.168.0.2/routerb-confg

How do you back up a Cisco router IOS?
To back up the current IOS image on your router, use the copy flash tftp privileged EXEC mode command:
RouterB#copy flash tftp
Source filename [routerb-flash]? flash:c2500-d-l.120-13.bin
Address or name of remote host []? 192.168.0.2
Destination filename [c2500-d-l.120-13.bin]?
!!
!!!6
897716 bytes copied in 90.856 secs (76641 bytes/sec)

How do you upgrade or restore the Cisco router IOS?
To upgrade or restore the Cisco router IOS, use the copy tftp flash privileged EXEC mode command.

How you make a Cisco router a TFTP server?
To configure a Cisco router as a TFTP server, use the tftp-server global configuration command.

What is the boot sequence of a Cisco router?
The boot sequence of a router is as follows:
hardware /power on
load run bootstrapfind the IOS software
load the softwarefind the config (default NVRAM)
load the configuration (startup-config) into RAM
Run the IOS

What can you configure on a router in setup mode?
ip addresses
routed protocols
enable password

Important Config Register Notes:
2100 manual boot rommon>
2101 boot from ROM

2102 normal/password recovery
2105 boot system command - config-register NVRAM
2142 bypass NVRAM
ctrl-break = ROM monitor mode
router(config)#boot system flash ios filename
router(config)#boot system tftp filename ip address
router(config)#boot system ROM

Note the router prompt for boot commands. Copy commands = router#

Quick Notes - IOS COMMANDS

What two EXEC modes are supported in the Cisco IOS?
The two EXEC modes are:
User EXEC mode (user mode)
Privileged EXEC mode (enable or privileged mode)

In the IOS, what is User EXEC mode?
User EXEC mode is the first mode you enter when you log into the IOS. This mode is limited and is mostly used to view statistics. You cannot change a router's configuration in this mode. By default, the greater-than sign (>) indicates that you are in user mode. This is how the router prompt looks in user mode:
Router>

In the IOS, what is privileged EXEC mode?
In privileged EXEC mode, you can view and change the configuration in a router. To enter privileged mode, enter the enable command while in user mode. The pound symbol (#) indicates that you are in privileged mode. This mode is usually protected with a password. You also see the output of the prompt:

Router>enable
Password:
Router#

When you are in privileged EXEC mode, how do you return to user EXEC mode?
You return to user EXEC mode using the disable, exit, or end IOS commands. Here is an example of using the disable command:

Router#disable
Router>

What two types of content-sensitive help are available in the Cisco IOS?
Word help and command syntax help are the two types of content-sensitive help. Word help uses a question mark and identifies commands that start with a character or sequence of characters. For example, the following router output shows the use of word help for any IOS command that starts with the letters cl:

Router#cl?
clear clock
Command syntax help is when you use a question mark after a command so that you can see how to complete the command.

For example:
Router#clock ?
set Set the time and date

On a Cisco router, what does the show version command display?

The show version command displays the system hardware's configuration, including RAM, Flash memory, software version, configuration register, and boot images. Here is an example of the show version command:

Router#show version
Cisco Internetwork Operating System SoftwareIOS (tm) 2500 Software (C2500-D-L), Version 12.0(13), RELEASE SOFTWARE (fc1)Copyright (c) 1986-2000 by Cisco Systems, Inc.Compiled Wed 06-Sep-00 01:08 by lindaImage text-base: 0x030388F8, data-base: 0x00001000 ROM: System Bootstrap, Version 5.2(5), RELEASE SOFTWAREBOOTFLASH: 3000 Bootstrap Software (IGS-RXBOOT), Version 10.2(5), RELEASE SOFTWARE (fc1) Router uptime is 50 minutesSystem restarted by power-onSystem image file is "flash:c2500-d-l.120-13.bin" cisco 2505 (68030) processor (revision C) with 8192K/2048K bytes of memory.Processor board ID 02073409, with hardware revision 00000000(text omitted)32K bytes of non-volatile configuration memory.8192K bytes of processor board System flash (Read ONLY) Configuration register is 0x2102

On a Cisco router, how do you display the configuration running in RAM?
You display the configuration running in RAM using the show running-config privileged mode command. For example:

Router#show running-config
Building configuration...
Current configuration:
!
version 12.0service timestamps debug uptimeservice timestamps log uptimeno service password-encryption
!
hostname Router
!
enable password cisco
!
--More--

On a Cisco router, how do you view the configuration stored in NVRAM?
You view the configuration stored in NVRAM using the show startup-config privileged mode command.

What Cisco router command would you use to view a list of the most recently used commands?
The show history command, by default, displays the last ten commands used. You can also use the up arrow key (or Ctrl-P) to display the last command you entered and the down arrow key (or Ctrl-N) to display the previous commands you entered. The following is an example of the show history command:

Router#show history
en

show running-config
show running-config
show history
enable
show version
show time
show history
Router#

Command history is enabled by default and records ten commands in its history buffer for the current session. How do you edit the number of commands that are stored in the router's history buffer?

To edit the number of command lines stored for the current session, use the terminal history [size number-of-lines] command in privileged EXEC mode. For example, the following changes the history size to 20 lines:

Router#terminal history size 20

Note: The maximum number of lines you can set for the current session is 256, but doing so wastes router memory. To turn off terminal history, use the terminal no history privileged mode command. If you want to set the history size longer than the current session, go to the console interface and enter the history [size number-of-lines] interface command as a more permanent way of changing the history buffer. This command is unavailable on a Catalyst 1900 switch.

On a Cisco router, name the enhanced editing commands that are used to do the following: ·

Move the cursor to the beginning of the line

· Move the cursor to the end of the line

· Move the cursor forward one character

· Move the cursor back one character

· Move the cursor back one word· Delete a line

· Complete a line· Display a line versus a screen

Move the cursor to the beginning of the line Ctrl-A

Move the cursor to the end of the line Ctrl-E

Move the cursor forward one character Ctrl-F

Move the cursor back one character Ctrl-B

Move the cursor back one word Esc-B

Delete all characters from the cursor to the beginning of the command line - Ctrl-U

Complete a line - Tab

Display a line versus a screen - Enter

What are global commands on a Cisco router?

Global configuration commands are commands that affect the entire router. They can be executed only in global configuration mode.

How do you enter global configuration mode?

To enter global configuration mode, you enter the config terminal command from

privileged EXEC mode. Here is an example of this command:
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#

How do you configure a name on a Cisco router?
The hostname name global configuration command is used to configure a name on a Cisco router. For example, the following command changes the router's host name to RouterA:
Router(config)#hostname RouterA
RouterA(config)#

How do you add a message-of-the-day (MOTD) banner on a Cisco router?
To add a message-of-the-day banner to a Cisco router, enter the banner motd # text # global configuration command. The pound signs (#) are delimiting characters. They can be any character of your choice, but they must be the same and cannot be included in your text. They signify the beginning and end of your text. The following example shows the banner motd command:
RouterA(config)#banner motd # Enter TEXT message. End with the character '#'.Warning only authorized users many access this Router. #
RouterA(config)#
Note: The MOTD banner is displayed to anyone connecting to the router via Telnet, console port, or auxiliary port.

On a Cisco router, how do you add a password to the console terminal?
To add a password to the console terminal, use the line console 0 global configuration command, followed by the login and password password line subcommands:
RouterA(config)#line console 0
RouterA(config-line)#login
RouterA(config-line)#password CCNA
In this example, the login subcommand forces the router to prompt for authentication. Without this command, the router will not authenticate a password. The password CCNA command sets the console password to CCNA. The password you set is case-sensitive.

How do you add a password for Telnet access on a Cisco router?
To add a password for Telnet access, enter the line vty 0 4 global configuration command, the login command, and finally the password line subcommand. The password is case-sensitive. In this example, the Telnet password is set to CCNA:
RouterA(config)#line vty 0 4
RouterA(config-line)#login
RouterA(config-line)#password CCNA

What command do you use to add a password to the auxiliary interface on your Cisco router?

To add a password to the auxiliary interface, use the line aux global configuration command, followed by the login and password subcommands. is the number of the auxiliary port you want to add a password to. The password is case-sensitive. The following example sets the password for the auxiliary port to CCNA:
RouterA(config)#line aux 0
RouterA(config-line)#login
RouterA(config-line)#password CCNA

On a Cisco router, how do you set a password to restrict access to privileged EXEC mode?
You set a password to restrict access to privileged EXEC mode using the enable password global configuration command:
RouterA(config)#enable password CCNA
This example sets the password to enter privileged mode to CCNA.

By default, when you view the router's configuration, the enable password is not encrypted. What command can you enter to use an encrypted enable password?
To use an encrypted enable password, use the enable secret password global configuration command, where password is a case-sensitive password you assign:
RouterA(config)#enable secret Cisco
If you have an enable password on your router, the IOS will allow you to use the same password as your enable password for your secret password, but this is not recommended. This is because the enable password is not encrypted and anyone can view it. If you have both an enable and secret password configured on your router, the router will use the secret password and not the enable password.
When you view the configuration on Cisco routers, only the enable secret password is encrypted.

How do you encrypt user mode and the enable password?
To encrypt user mode and the enable password, use the service password-encryption global command:

RouterA(config)#service password-encryption

How do you configure Cisco router interfaces?
To configure an interface on a Cisco router, use the interface interface-type number global command, where interface-type number is the interface type and number you want to configure. For example, if you want to configure the second serial interface on your router, you would enter the following:
RouterA(config)#interface serial 1
RouterA(config-if)#
Cisco interfaces start with 0 instead of 1. So the first interface would be number 0. The prompt also changes to RouterA(config-if)# to tell you that you are in interface mode. If you have a router with module slot, such as the Cisco 3600,

you would enter into interface mode by entering the slot/port number. For example, if you have a Cisco 3600 router with two module serial interfaces and you want to configure the first serial interface on the second module you would enter interface s1/0.

How do you administratively disable an interface on a Cisco router?
You administratively disable an interface on a Cisco router by issuing the shutdown interface configuration command. In this example, the serial interface is issued the shutdown command: RouterA(config)#int s0
RouterA(config-if)#shutdown
00:27:14: %LINK-5-CHANGED: Interface Serial0, changed state to administratively down
To administratively enable an interface, use the no shutdown interface command.

What are some of the things the show interface interface-type number command displays?
The show interface command displays the following: · Whether the interface is administratively down· Whether the line protocol is up or down· An Internet address (if one is configured)· MTU and bandwidth· Traffic statistics on the interface· Interface encapsulation type

RouterA#show interface s0
Serial0 is down, line protocol is down
Hardware is HD64570 Internet address is 192.168.1.1/24 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255 Encapsulation HDLC, loopback not set, keepalive set (10 sec) Last input never, output never, output hang never Last clearing of "show interface" counters never Input queue: 0/75/0 (size/max/drops); Total output drops: 0 Queueing strategy: weighted fair Output queue: 0/1000/64/0 (size/max total/threshold/drops) Conversations 0/0/256 (active/max active/max total) Reserved Conversations 0/0 (allocated/max allocated) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 0 packets input, 0 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort 0 packets output, 0 bytes, 0 underruns 0 output errors, 0 collisions, 2 interface resets 0 output buffer failures, 0 output buffers swapped out 0 carrier transitions DCD=up DSR=up DTR=down RTS=down CTS=up

On your Cisco router, you enter show interface s0 and notice that the port is administratively down. What does this mean, and how do you fix it?
When an interface is administratively down, it has been shut down manually. To remedy this, enter the interface command no shut.

What two commands can you use to show the clock rate on a serial interface?
To view the clock rate on a serial interface, you can use the show running-config enable command and the show controllers enable command.

Assuming that you are using no CSU/DSU and you are using back-to-back DTE/DCE serial cables, what command would you use to set the serial interface on a router to provide clocking to another router at 64 Kbps?

The command to set the serial interface on a router to provide clocking to another router at 64 Kbps is clock rate 64000. Setting the clock rate on an interface makes it a DCE interface.

What Cisco IOS router command would you use to find out whether a serial interface is a DCE or DTE interface (providing clocking)?

To see whether a serial interface is providing clocking, use the enable command show controllers serial-interface-type serial-number. The following example shows that serial interface 0 is providing clock rate at 56 Kbps:

RouterA#show controllers s 0
HD unit 0, idb = 0xCCE04, driver structure at 0xD2298buffer size 1524 HD unit 0, V.35 DCE cable, clockrate 56000cpb = 0x81, eda = 0x4940, cda = 0x4800RX ring with 16 entries at 0x814800

Quick Notes - PPP

PPP can be used over what physical WAN interfaces?

PPP can be used on the following:
Asynchronous serial interfaces
High-Speed Serial Interface (HSSI)
ISDN
Synchronous serial interfaces

PPP is a data link layer protocol that provides network-layer services. What are the two sublayers of PPP?

The two sublayers of PPP are the following:
Network Core Protocol (NCP) is the component that encapsulates and configures multiple network layer protocols. Some examples<>
Link Control Protocol (LCP) is used to establish, configure, maintain, and terminate PPP connections.

What features does LCP offer to PPP encapsulation?

LCP offers authentication, callback, compression, error detection, and multilink to PPP encapsulation.
The two methods of authentication on PPP links are:
Password Authentication Protocol (PAP)
Challenge Handshake Authentication Protocol (CHAP)
PAP is the less-secure of the two methods; passwords are sent in clear text and are exchanged only upon initial link establishment.
CHAP is used upon initial link establishment and periodically to make sure that the router is still communicating with the same host. CHAP passwords are exchanged as MD5 encrypted values.

What two protocols are available for compression on PPP links?

The two protocols available for compression are Stacker and Predictor.

What three phases are used to establish a PPP session?

The three phases used to establish a PPP session are the following:
Step 1. Link establishment--Each PPP device sends LCP packets to configure and test the link (Layer 1).
Step 2. Authentication phase (optional)--If authentication is configured, either PAP or CHAP is used to authenticate the link. Authentication must take place before the network layer protocol phase can begin (Layer 2).
Step 3. Network layer protocol phase--PPP sends NCP packets to choose and configure one or more network layer protocols to be encapsulated and sent over

the PPP data link (Layer 3).
Note on authentication: Hostname and passwords are case-sensitive.

How do you enable PPP encapsulation on a Cisco router serial interface?

To enable PPP encapsulation on a serial interface, enter the encapsulation ppp interface command:
RouterB(config-if)#encapsulation ppp

How do you enable PPP authentication using PAP or CHAP on a Cisco router?
To enable PPP authentication on a Cisco router, follow these steps:
Step 1. Make sure that each router has a host name assigned to it using the hostname command.
Step 2. On each router, define the username of the remote router and password that both routers will use with the username name password password command.
Step 3. Configure PPP authentication with the ppp authentication {chap chap pap pap chap pap} interface command. (If both PAP and CHAP are enabled, the first method you specify in the command is used. If the peer suggests the second method or refuses the first method, the second method is used.)
For example:
RouterB(config)#hostname RouterB
RouterB(config)#username RouterA password cisco
RouterB(config)#int s0
RouterB(config-if)#ppp authentication chap pap

What is the default encapsulation on a Cisco serial interface?

HDLC

Quick Notes - ISDN

In ISDN, what do E-series protocols specify?
E-series protocols specify telephone network standards for ISDN. Examples include International ISDN addressing and the International Telephone plan.

What do protocols that begin with I deal with?
I-series protocols deal with concepts, terminology, and general methods of ISDN, such as service aspects, user network interfaces, and network aspects.

What do ISDN protocols that begin with Q specify?
Q-series protocols specify how switching and signaling (call setup) should operate. For example, ISDN protocol Q.921 is used for LAPD on the D channel, and protocol Q.931 is used for the ISDN network layer between the terminal and switch.

What is the data transfer speed for ISDN BRI?
The data transfer rate for ISDN BRI is 128 Kbps. The total transfer rate for ISDN BRI is 144 Kbps. This consists of two 64 Kbps (128 Kbps) Bearer (B) channels plus one 16 Kbps Delta (D) channel. The B channels can be used for data transfer and voice transmission. The D channel carries control and signaling information for fast call setup and operates at the first three layers of the OSI model.

What is the total rate in Mbps for ISDN PRI?
The total rate for ISDN PRI in the U.S. and Japan is 1.544 Mbps. PRI consists of 23 64 Kbps B channels and one 64 Kbps D channel. In Europe, PRI consists of 30 B channels and one D channel for a total rate of 2.048 Mbps.
In ISDN, the D channel appears to always be up and is what makes the call to the ISDN switch.

What signaling protocol does the ISDN switch use to set up a path and pass the called number to the terminating ISDN switch?
The ISDN local switch uses the SS7 protocol to set up a path and pass the called number to the terminating ISDN switch.

Devices connecting to an ISDN network are known as terminal equipment (TE) and network termination (NT) equipment. What do the TE1 and TE2 equipment types refer to?
TE1 refers to a device that has a native ISDN interface. That is, it can plug directly into an ISDN network. TE2 refers to equipment that does not have an ISDN interface and that requires a terminal adapter (TA) to plug into an ISDN network.

To what do ISDN NT1 and NT2 termination types refer?
Network Terminal 1 converts BRI signals into a form used by the ISDN line. It

implements the physical layer specifications and connects the devices to the ISDN network. NT2 is the point where all ISDN lines are aggregated and switched using a customer-switching device.

What is the function of the TA?
The terminal adapter converts non-ISDN signals into ISDN signals. Devices that are not native to ISDN connect to a TA to access the ISDN network.

What does the ISDN R reference point define?
The R reference point defines the point between a non-ISDN-compatible device and a TA.

What does the ISDN S point reference?
The S point references the points or customer equipment that connects to the NT2 or customer-switching device.

What does the ISDN T reference point define?
ISDN T reference points refer to the point between NT1 and NT2 devices. T and S reference points are electronically the same and reference the outbound connection from the NT2 to the ISDN network.

What is the ISDN U reference point?
The U reference point is the point between the NT1 and the ISDN network.

What happens when you connect a router with a U interface into an NT1?
If you connect a router with a U interface into an NT1, you will damage the interface. This is because the U interface on a Cisco router already has a built-in NT1.

What are SPIDs?
Service provider or profile identifiers (SPIDs) are used to identify your router to the switch at the central office (the ISP). They are a series of characters that look like phone numbers and are not always required.

How do you enable ISDN on a Cisco router?
To enable ISDN on a Cisco router, first you need to define the switch type your router will be connecting to. The switch type is the type of switch used by your service provider. To define the ISDN switch type, enter the isdn switch-type switch-type global or interface command. Specifying the isdn switch-type global command specifies the ISDN switch type for the entire router. The second step is to enter the SPIDs provided by your service provider by entering the isdn spid1 spid-number and isdn spid2 spid-number interface commands. The following example enables ISDN on a router, specifying AT&T basic-rate switches as the switch type:

```
RouterA(config-if)#isdn switch-type basic-5ess
RouterA(config-if)#isdn spid1 123456789123
```

RouterA(config-if)#isdn spid2 123456789124

If you have DDR enabled on your router, when does the router decide when to bring up the ISDN line and send traffic?

If DDR is enabled on your router, it brings up the ISDN line when it sees "interesting traffic".

How do you enable DDR on a Cisco router?

To enable DDR on a Cisco router, you first need to define static routes with the ip route command. Next, specify interesting traffic, and finally, configure the dialer information.

How do you specify interesting traffic?

As an administrator, you define that interesting traffic can be based on protocol type or addresses for source or destination hosts. To define interesting traffic, use the following command: dialer-list dialer-group protocol protocol-name {permit deny list access-list-number}

dialer-group is the number that identifies the dialer list. protocol-name can be IP, IPX, AppleTalk, DECnet, or Vines.

RouterA(config)#dialer-list 10 protocol ip list 100
RouterA(config)#access-list 100 permit tcy any any eq www
RouterA(config)#access-list 100 permit tcy any any eq smtp
RouterA(config)#access-list 100 permit tcy any any eq dns

The last step in configuring DDR on a Cisco router is to configure the dialer information. How do you do this?

Do the following to configure the dialer information:

Step 1. Choose the interface.
Step 2. Configure an IP address on the interface.
Step 3. Configure the encapsulation type.
Step 4. Bind interesting traffic to the interface by using the dialer-group group-number interface command.

What command can you use to view the call in progress?

The show isdn active command shows the call in progress and the number dialed:

show isdn st
RouterA#Global ISDN Switchtype = basic-5ess
ISDN BRI0 interface dsl 0, interface ISDN Switchtype = basic-5ess
Layer 1 Status:
ACTIVE
Layer 2 Status: TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
Layer 3 Status: 0 Active Layer 3 Call(s) Activated dsl 0 CCBs = 0
The Free Channel Mask: 0x80000003
Total Allocated ISDN CCBs = 0

How can you view the number of times the dial string has been successfully reached on a Cisco router?

The show dialer command displays information about the interface configured for DDR, the number of times the dialer string has been successfully reached, and the fast and idle timer values for each B channel.

Quick Notes - VLANS

What are VLANs?
VLANs are broadcast domains in a Layer 2 network. Each broadcast domain is like a distinct virtual bridge within the switch. Each virtual bridge you create in a switch defines a broadcast domain. By default, traffic from one VLAN cannot pass to another VLAN. Each of the users in a VLAN is also in the same IP subnet, and each switch port can belong to only one VLAN.

What are the three characteristics of a typical VLAN setup?
The three characteristics of a typical VLAN setup are:
Each logical VLAN is like a separate physical bridge.
VLANs can span multiple switches.
Trunks carry traffic for multiple VLANs.

What are trunk links?
By default, each port on a switch can belong to only one VLAN. For devices that are in VLANs (that span multiple switches) to talk to other devices in the same VLAN, you must use trunking or have a dedicated port per VLAN. Trunk links allow the switch to carry multiple VLANs across a single link.

What are the two methods you can use to assign a port to a VLAN?
The two methods to assign a port to a VLAN are
Statically
Dynamically

What is Inter-Switch Link (ISL)?
ISL is a Cisco proprietary protocol used to interconnect switches that have multiple VLANs. It maintains VLAN information as traffic goes between switches, allowing the traffic to enter the correct VLAN. ISL operates in a point-to-point environment.

At which layer of the OSI model does ISL function?
ISL functions at Layer 2 of the OSI model. It encapsulates a data frame with a new ISL header and CRC. Because ISL operates at Layer 2 of the OSI model, it is protocol-independent.

What type of tagging method does ISL use?
Many network professions refer to the way ISL tags frames as an external tagging mechanism. This is because ISL encapsulates each frame and does not modify the original packet.
Many network professions refer to the way ISL tags frames as an external tagging mechanism. This is because ISL encapsulates each frame and does not modify the original packet.

How many extra bytes does ISL add to an existing Ethernet frame?

ISL adds a 26-byte ISL header and a 4-byte CRC to each frame, extending each Ethernet frame by 30 bytes. ISL tagging is implemented in ASICs, so tagging is done at wire speed.

What is VTP?
VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency throughout a common administrative domain by managing VLANs' additions, deletions, and name changes across multiple switches. Without VTP, you would have to add VLAN information in all switches in your network.

What is a VTP domain?
A VTP domain is one or more interconnected switches that share the same VTP environment. A switch can be in only one VTP domain, and all VLAN information is propagated to all switches in the same VTP domain.

What are the three VTP modes?
The three VTP modes are
Server
Client
Transparent

What is VTP server mode?
A switch in VTP server mode can add, delete, and modify VLANs and other configuration parameters for the entire VTP domain. This is the default mode for all Catalyst switches. VLAN configurations are saved in NVRAM. When you change VLAN configuration in server mode, the change is dynamically propagated to all switches in the VTP domain.

What is VTP client mode?
In VTP client mode, a switch cannot create, delete, or modify VLANs. Also, a VTP client does not save VLAN information and configuration in NVRAM. In client and server mode, VLAN information is synchronized between switches in the VTP domain.

What is VTP transparent mode?
In transparent mode, a switch can add, modify, and delete VLANs. This information is not transmitted to other switches in the VTP domain. They affect only the local switch. VTP transparent mode is used when a switch does not need to participate in the VTP domain but needs to propagate VTP information to other switches.

How often are VTP advertisements flooded throughout the management domain?
VTP advertisements are flooded throughout the management domain every 5 minutes or whenever a change occurs in VLAN configuration.

What is included in VTP advertisements?
VTP advertisements include the following:
VTP revision number
VLAN names and numbers
Information about switches that have ports assigned to each VLAN

What is one of the most important components of the VTP advertisement?
The revision number is one of the most important components of the VTP advertisement. Every time a VTP server modifies its VLAN configuration, it increments the configuration number by 1. The largest configuration number in the VTP domain contains the most current information. When a client receives a revision number higher than its current number, it updates its VLAN configuration.

On a Catalyst 1900 switch, how do you reset the configuration number?
To reset the configuration numbers on a Catalyst 1900, use the delete vtp privileged EXEC command, and then reset the switch.

What is VTP pruning?
By default, a trunk link carries traffic for all VLANs in the VTP domain. Even if a switch does not have any ports in a specific VLAN, traffic for that VLAN is carried across the trunk link. VTP pruning uses VLAN advertisements to determine when a trunk connection is needlessly flooding traffic to the trunk links that the traffic must use to access the appropriate network device.

How many VLANs with a separate spanning tree per VLAN does the Catalyst 1900 support?
The Catalyst 1900 supports 64 VLANs with a separate spanning tree per VLAN.

What VLAN number are CDP and VTP advertisements sent across?
CDP and VTP advertisements are sent on VLAN 1, which is also known as the management VLAN.

What must you remember before you create VLANs on a Catalyst switch?
Before you create VLANs on a Catalyst 1900 switch, the switch must be in VTP server mode or VTP transparent mode.

How do you configure the VTP operation mode on a Catalyst 1900?
To configure VTP on a Catalyst 1900, use the vtp [server transparent client] global configuration command:
Cat1900(config)#vtp server

How do you configure a VTP domain on a Catalyst 1900 switch?
To configure a VTP domain on a Catalyst 1900 switch, use the vtp domain domain-name global command:

Cat1900(config)#vtp domain cisco

How do you configure a VTP domain password on a Catalyst 1900?
Use the vtp password password global command to configure a VTP domain password. This example sets the VTP password to cisco:
Cat1900(config)#vtp password cisco

What does the show vtp privileged EXEC command display?
The show vtp privileged EXEC command displays the following:
VTP version
The number of existing VLANs on a switch and the maximum number of locally supported VLANs
VTP domain name, password, and operating mode
Whether VTP pruning is enabled
The last time VLAN configuration was modified.
Here's an example of show vtp output:

Cat1900#show vtp
VTP version: 1
Configuration revision: 0
Maximum VLANs supported locally: 1005
Number of existing VLANs: 5
VTP domain name : cisco
VTP password : cisco
VTP operating mode : Server
VTP pruning mode : Disabled
VTP traps generation : Enabled
Configuration last modified by: 192.168.0.2 at 00-00-0000 00:00:00

What command do you use to add a VLAN on a Catalyst switch?
To add a VLAN on a Catalyst switch, use the vlan vlan-number [name vlan_name] global command. The following example adds VLAN 10 with a name of Sales: Cat1900(config)#vlan 10 name Sales

What Catalyst 1900 command can you use to verify VLAN information?
To verify VLAN information, use the show vlan vlan-number privileged EXEC command.

How do you view spanning tree information for a particular VLAN?
A Catalyst 1900 switch can have a maximum of 64 VLANs with a separate instance of spanning tree per VLAN. To view spanning tree information for a particular VLAN use the "show spandtree vlan-id" command.

Quick Notes - TCP / IP

What are the four layers of the TCP/IP layer model?

The four layers of the TCP/IP layer model are:
Application (process)
Host-to-host (transport)
Internet
Network Access (physical and data link)

What two protocols function at the transport (host-to-host) layer of the TCP/IP model?

The two protocols that function at the host-to-host layer of the TCP/IP model are TCP and UDP. (TCP is a connection-oriented, reliable protocol. UDP is a connectionless and unacknowledged protocol.)

What are the protocol numbers for TCP and UDP?

The protocol number for TCP is 6. The protocol number for UDP is 17.

How many bytes are in the header for TCP and UDP packets?

A TCP header contains 20 bytes, and a UDP header contains 8 bytes.

What are TCP and UDP port numbers?

To pass information (such as e-mail) to upper layers, TCP and UDP use port numbers. These port numbers are used to keep track of different conversations among different hosts at the same time. Originating source port numbers are dynamically assigned by the source host, which is a number greater than 1023.

What is the number range for "well-known" port numbers?

Defined in RFC 1700, the well-known port numbers are 1 to 1023.

What are the steps for the TCP three-way handshake?
The steps for the TCP three-way handshake are as follows:
Step 1. The source host sends a SYN to the destination host.
Step 2. The destination host replies with a SYN/ACK to the source host.
Step 3. The source host replies with an ACK.

What are some protocols that operate at the TCP/IP Internet layer?

Some protocols that operate at the TCP/IP Internet layer are
IP

ICMP
ARP
RARP

What is the Internet Protocol (IP)?

IP is a connectionless protocol that provides best-effort delivery routing of datagrams.

What is the Internet Control Message Protocol (ICMP)?

ICMP is a management protocol for IP. ICMP messages are carried in IP datagrams and are used to send error and control messages. An example of a utility that uses ICMP is ping.

What is the Address Resolution Protocol (ARP)?

ARP is used to resolve a known IP address to a MAC address. In order for a host to communicate with another host, it must know the MAC address of the destination host (if they are on the same network) or next hop router. This is the reason for ARP.

What is the Reverse Address Resolution Protocol (RARP)?

RARP is a protocol used to find the IP address of a station that knows its MAC address. It is mainly used for diskless workstations that boot up and need an IP address. An RARP request is a broadcast packet.

What are the IP address ranges for Class A, Class B, and Class C addresses?

The address ranges are as follows: Class A 1.0.0.0 to 126.0.0.0Class B 128.0.0.0 to 191.255.0.0Class C 192.0.0.0 to 223.255.255.0

What does RFC 1918 define?

RFC 1918 defines reserved (private) networks and addresses that are not routed on the Internet. These addresses are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. They are used as internal private addresses. Private addresses are widely used today, along with proxy servers and Network Address Translation to assist with "stretching" the current IP address space.

Cisco IOS software supports what three kinds of broadcasts?

The three kinds of broadcasts that Cisco IOS software supports are:
Flooding

Directed broadcast
All-subnet broadcast
Flooded broadcasts are local broadcasts that have an address of 255.255.255.255. They are not propagated by a router.
Direct broadcasts are directed to a specific network. They contain all 1s in the host portion of the address. Routers forward these broadcasts. An example is 192.168.0.255/24.
All-subnet broadcast are broadcast messages to all hosts within a subnet and to all subnets within a network. An example is 192.168.255.255/24. With Cisco IOS release 12.0, a router does not forward all subnet broadcasts. You can use the ip directed-broadcast command to enable all subnet broadcasts.

How do you assign an IP address to a Cisco router?

To assign an IP address to a router, use the ip address address subnet-mask interface configuration command. Here's an example:
RouterB(config)#inter e0
RouterB(config-if)#ip address 172.16.0.1 255.255.0.0
RouterB(config-if)#no shut
Note: By default all interfaces on a Cisco router are administratively disabled. To enable them you must use the "no shut" interface command.

How do you manually assign IP addresses to host names in a Cisco router?

The ip host name [tcp-port-number] address [address] global configuration command lets you assign IP addresses to host names in a Cisco router. [tcp-port-number] is an optional parameter; the default value is Telnet. Here's an example:
RouterB(config)#ip host cisco 172.16.0.1

What Cisco IOS command can you use to program the router to use a DNS server to resolve host names?

The ip name-server server-address [[server-address2]...[server-address6]] command lets you program the Cisco router to resolve host names with a DNS server. Here's an example:
RouterB(config)#ip name-server 172.16.0.250

If you enter a command that a Cisco router does not recognize, the router tries to resolve the command you just entered with a DNS server. How do you turn off this DNS domain lookup?

To turn off DNS domain lookup, use the no ip domain-lookup global command.

Here's an example: RouterB#enb
Translating "enb"...domain server (255.255.255.255)% Unknown command or computer name, or unable to find computer address
RouterB#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterB(config)#no ip domain-lookup

For different VLANs to communicate with each other, they need to be routed (a router!). To perform inter-VLAN routing, what two things must occur?

To perform inter-VLAN routing, the following must occur:
The router must know how to reach all VLANs being interconnected.
The router must have a separate physical connection on the router for each VLAN, or trunking must be enabled on a single physical connection.

How do you enable ISL trunking on a Cisco router?

To enable ISL trunking on a Cisco router, you must do the following:
Step 1 Configure subinterfaces on the router's physical Fast Ethernet or Gigabit interface. (ISL trunking works only on Fast Ethernet or Gigabit interfaces.)
Step 2 Assign an IP address to the subinterface.
Step 3 Enable ISL encapsulation for the particular VLAN with the encapsulate isl vlan# subinterface command.
Here's an example:

RouterB(config)#int f0/0
RouterB(config-subif)#ip address 172.16.0.1 255.255.0.0
RouterB(config-subif)#encapsulation isl 1