STUDY GUIDE

Cisco

640-822

CCNA ICND (Part I)

ExamForce

About the Exam

The Introduction to Cisco Networking Technologies exam is one of the two qualifying exams available to those who want to pursue a two-exam option for CCNA. The exam will certify that the successful candidate has the knowledge and skills necessary to describe and identify major network and WAN components along with their function and purpose. There are seven major topic areas that make up this exam:

- Describe the operation of data networks
- Implement a small switched network
- Implement an IP addressing scheme and IP services to meet network requirements for a small branch office
- Implement a small routed network
- Explain and select the appropriate administrative tasks required for a WLAN
- Identify security threats to a network and describe general methods to mitigate those threats
- Implement and verify WAN links

This guide will walk you through all the skills measured by the exam, as published by Cisco.

Objectives

Chapter 1: Describe the operation of data networks

Describe the purpose and functions of various network devices.

Select the components required to meet a given network specification.

Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network.

Describe common networking applications including web applications.

Describe the purpose and basic operation of the protocols in the OSI and TCP models.

Describe the impact of applications (Voice Over IP and Video Over IP) on a network.

Interpret network diagrams.

Determine the path between two hosts across a network.

Describe the components required for network and Internet communications.

Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach.

Differentiate between LAN/WAN operation and features.

Chapter 2: Implement a small switched network

Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts.

Explain the technology and media access control method for Ethernet technologies.

Explain network segmentation and basic traffic management concepts.

Explain the operation of Cisco switches and basic switching concepts.

Perform, save and verify initial switch configuration tasks including remote access management.

Verify network status and switch operation using basic utilities (including: ping, traceroute, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands.

Implement and verify basic security for a switch (port security, deactivate ports.)

Identify, prescribe, and resolve common switched network media issues, configuration issues, autonegotiation, and switch hardware failures.

Chapter 3: Implement an IP addressing scheme and IP services to meet network requirements for a small branch office

Describe the need and role of addressing in a network " Create and apply an addressing scheme to a network.

Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment.

Explain the basic uses and operation of NAT in a small network connecting to one ISP.

Describe and verify DNS operation.

Describe the operation and benefits of using private and public IP addressing.

Enable NAT for a small network with a single ISP and connection using SDM and verify operation using CLI and ping.

Configure, verify and troubleshoot DHCP and DNS operation on a router (including: CLI/SDM).

Implement static and dynamic addressing services for hosts in a LAN environment.

Identify and correct IP addressing issues.

Chapter 4: Implement a small routed network.

Describe basic routing concepts (including: packet forwarding, router lookup process.)

Describe the operation of Cisco routers (including: router bootup process, POST, router components.)

Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts.

Configure, verify, and troubleshoot RIPv2.

Access and utilize the router CLI to set basic parameters.

Connect, configure, and verify operation status of a device interface.

Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities.

Perform and verify routing configuration tasks for a static or default route given specific routing requirements.

Manage IOS configuration files (including: save, edit, upgrade, restore.)

Manage Cisco IOS.

Implement password and physical security.

Verify network status and router operation using basic utilities (including: ping, traceroute, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands.

Chapter 5: Explain and select the appropriate administrative tasks required for a WLAN

Describe standards associated with wireless media (including: IEEE WI-FI Alliance, ITU/FCC.)

Identify and describe the purpose of the components in a small wireless network. (including: SSID, BSS, ESS.)

Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point.

Compare and contrast wireless security features and capabilities of WPA security (including: open, WEP, WPA-1/2.)

Identify common issues with implementing wireless networks.

Chapter 6: Identify security threats to a network and describe general methods to mitigate those threats

Explain today's increasing network security threats and the need to implement a comprehensive security policy to mitigate the threats

Explain general methods to mitigate common security threats to network devices, hosts, and applications

Describe the functions of common security appliances and applications

Describe security recommended practices including initial steps to secure network devices

Chapter 7: Implement and verify WAN links

Describe different methods for connecting to a WAN

Configure and verify a basic WAN serial connection

Chapter 1 - Describe the Operation of Data Networks

Quick Jump To:

- Chapter 1
- Chapter 2
- Chapter 3
- Chapter 4
- Chapter 5
- Chapter 6
- Chapter 7

Describe the purpose and functions of various network devices.

Network Interface Cards, often called NICs for short, are one of the most commonly used and preferable methods of attaching devices to a network. A NIC is nothing more than an expansion board for a PC that is installed to provide access to the local network. If operating on a 100Mbps fast Ethernet LAN, it is necessary to purchase a card compatible with the LAN requirements. Also, it is also imperative to know what the type of LAN; a Token Ring NIC is very different from an Ethernet NIC.

NOTE: Every NIC is manufactured with a unique identifier called a MAC address. Most times, the first half of the MAC address is the vendor ID, and the second half is the unique identifier. Every MAC address on a network needs to be unique because the MAC address is what is resolved via Arp resolution traffic between the nodes. If a duplicate exists, then there is a conflict, which means that one node will not be able to transmit. This is why the NIC has what is called a BIA (Burned in Address) so that each one can be unique.

Router is the device responsible for forwarding data packets along networks. On networks with a mesh configuration, multiple paths exist and the router has to look for the best possible path (via packet headers and forwarding tables) on behalf of its users. For a router to be useful, it has to be connected to at least two networks. This is why routers are typically located at gateways where the networks connect.

Switches are data link layer devices that enable multiple physical LAN segments to be interconnected. Simply put, a larger LAN can be built through switching. A big LAN may be segmented into smaller ones through switching.

To effectively prepare for the CCNA exam, it is recommended to have hands on experience using the "real steel". This experience is necessary both for the exam and for upcoming job interviews.

A typical lab setup recommended for CCNA/CCNP preparation may include several routers (such as the 2500 and the 3000) together with at least one Catalyst switch. You need these gears to setup a small network for testing out the various functions covered in the exams.

NOTE: Keep in mind that routing takes place at layer 3, and switching in general takes place at layer 2, although Cisco now supports multi-layer switching on certain devices.

Select the components required to meet a given network specification.

Formally speaking, networks are made up of four basic components, which are Protocols, Transmission media, NOS (Network Operating System) and Shared resources. There are two major types of networks - peer-to-peer and server-based. Peer-to-peer networks are used in many households and in small companies. Each computer in a peer-to-peer network can both share and use resources like files and printers. A Server based network is quite the opposite of a peer to peer. It allows for more hosts, it has a solid security model and is scalable. It revolves around a

model that the end users attach to a security domain that allows control over centralized resources.

From the Cisco perspective, designing a simple LAN with Cisco products involves primarily the deployment of the Catalyst switches along a Star topology. Cisco does not provide Server based NOS nor desktop clients – those are the responsibilities of Windows and Linux.

A Star Topology is physical network topology that has all connections terminating into a centralized concentrator. A switch has all devices centrally connect to a device that will record its MAC address after the flooding stage, once completed; each device can communicate with other devices on the Star.

Since switching is performed in hardware rather than in software, it is significantly faster than, say, routing. Most switches use either a store-and-forward switching mechanism or a cut-through switching mechanism when forwarding traffic.

LAN switching technology employs micro-segmentation for further segmenting the LAN ultimately to a single user with a dedicated LAN segment. Each switch port provides a dedicated full speed Ethernet segment.

A LAN switch can enable communication between LANs while blocking other types of traffic. It has the intelligence of monitoring traffic and compiling address tables so that traffic can be forwarded to the specific ports. If necessary it can be configured to provide non-blocking service so that multiple conversations can occur simultaneously. Superior throughput performance, higher port density, lower per-port cost, and greater flexibility are the advantages offered by LAN switches over bridges and hubs.

When implementing a wired LAN it is important to realize that the trend now is to implement switched LAN rather than shared LAN. A shared LAN using hubs and repeaters is no longer preferred. Instead, switching technology is quickly becoming the de-facto standard for improving LAN traffic due to the following reasons:

- Switches allow multiple data streams to pass simultaneously.
- Through microsegmentation, switches can support the increased speed and bandwidth requirements of emerging network technologies.
- Switches can deliver dedicated bandwidth to users through high-density group switched and switched 10BaseT or 100BaseT Ethernet, flexible 10/100 BaseT Ethernet, fiber-based Fast Ethernet, Fast EtherChannel, Token Ring, CDDI/FDDI, and ATM LAN Emulation (LANE).

For an in-depth explanation of the routing function see Chapter 4. For an in-depth description of the various security devices see Chapter 6 Objective 3.

Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network.

As the industry standard way of shaping the networking process, the OSI model actually defines a framework for implementing protocols in seven layers in such a way that control is passed from one layer to the next, station to station. The Application layer is at the top of the hierarchy, while the Physical layer is at the bottom.

7.	Application
6.	Presentation
5.	Session
4.	Transport
3.	Network
2.	Data Link
1.	Physical

The Application Layer is responsible for identifying and establishing the availability of desired communication partner and verifying sufficient resources exist for communication. Protocols such as HTTP, SMTP and FTP work at this layer.

Also known as the syntax layer, the Presentation Layer is responsible for presenting the data in standard formats and provides services such as data compression, decompression, encryption, and decryption. Some of the well-known standards at this layer are JPEG, MPEG, MIDI, PICT, Quick Time, and TIFF.

The Session Layer is responsible for coordinating communication between network nodes. Simply put, it deals with session and connection coordination. Well known session layer protocols and interfaces include NFS, SQL and RPC.

The Transport Layer is responsible for flow control, with the primary aim of maintaining data integrity. Simply put, it works to ensure complete data transfer.

The Network Layer has the primary responsibility of sending data packets from the source network to the destination network using a pre-specified routing method. Most routers work at this layer.

The Data Link Layer is divided into the sub-layers of Logical Link Control (LLC) and Media Access Control (MAC). The LLC sub-layer handles tasks such as error control, flow control and framing, while the MAC sub-layer handles access to shared media.

The Physical Layer is where the actual flow of signals is taking place. At this layer, the physical interface between the DTE and DCE is determined. Note that protocols such as Fast Ethernet, RS232, and ATM all include components that function at this level.

TCP/IP has its own 4-layer model that corresponds to the layers in the OSI model. Most of the time, however, we go with the OSI model.

NOTE: For the CCNA exam you will need to know what devices operate at which layer of the OSI model. For exam, you will need to know that a router operates at Layer 3. You will also need to know what protocols operate at which layers of the OSI model. For exam, WAN protocols such as Frame Relay operate at Layer 2 (the Data Link layer) of the OSI model.

Describe common networking applications including web applications. Describe the purpose and basic operation of the protocols in the OSI and TCP models.

SSL

Web applications run mostly through HTTP and SSL. Netscape developed SSL for transmitting private documents over the Internet. This technology works by using a private key to encrypt data that is transferred over the secured connection. Since a secure connection is established between the client and the server, any amount of data may be sent securely through the connection. Note that URLs that require an SSL connection start with "https:".

Telnet, FTP and TFTP

The most commonly used protocols for establishing connectivity from the console to the remote devices are Telnet, FTP and TFTP, which are all considered as client-server protocols.

As a common way to remotely control network devices, Telnet refers to the terminal emulation program for TCP/IP networks, which requires that logging in with a valid password for access. One major problem with Telnet is security – password is transmitted in clear text and is therefore subject to security attack of different kinds.

To access a Cisco router remotely with Telnet, from the remote host enter the telnet command and then designate the name or IP address of the router in order to connect to it. Then, at the prompt, enter the password necessary for gaining access. Once authenticated, enter the necessary commands to complete the desired tasks.

FTP is a file transfer protocol which is connection oriented. It is different from TFTP in that FTP works using the connection oriented TCP, while TFTP works using the connectionless UDP. Due to the connectionless nature, UDP provides very few error recovery services but instead offers a very direct way to send and receive datagrams over an IP network. It is therefore making

TFTP more efficient performance-wise. The TCP based FTP, on the other hand, is more reliable but is having more overheads.

Anonymous FTP, which requires no username and password for access, can be allowed. The safer way of establishing connectivity, however, is to enforce the use of username and password:

- To configure the username for FTP connections, use the "ip ftp username" global configuration command. On the other hand, to configure the router to attempt anonymous FTP, use the no form of this command.

- To specify the password to be used for FTP connections, use the "ip ftp password" global configuration command.

When running TFTP on a network, there is a need to configure a TFTP server. To configure a Cisco router as a TFTP server, use the different variations of the "tftp-server" global configuration command.

SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol for distributed network management. It facilitates the exchange of management information between network devices. It is quite helpful, as it can be used to manage network performance, find and solve network problems, and plan for network growth. There are currently two versions of SNMP, and standardization of version three is pending.

Voice and Video Traffics

In the past, design concern is solely on data. However, voice and multimedia/video networking must also be taken into account. That is, the topic of convergence needs to be addressed. Refer to the next chapter for further information.

Describe the impact of applications (Voice Over IP and Video Over IP) on a network.

Voice over IP (VoIP) networks rely on the H.323 standard for transmitting real-time audio communications over packet-based networks. Identify the VoIP characteristics and ensure that the requirements for successful implementation are present.

NOTE:	H.225 is a standard about call control signaling. It setups connections in between two H.323 endpoints. It also specifies the use of Q.931 based signaling messages. With H.225, a TCP based call control channel can be created through the TCP port #1720. Through this port the various Q.931 call control messages may be initiated.

It is important to characterize what the conditions are now and then find out what is to be expected after new implementations. The first step in analysis effort is to gather information on voice usage. The following information is critical:

- The organization's existing social requirements on voice communication
- The network owner's current voice network and future needs

The following questions may naturally arise:

1. Where do the network gears spend their time?
2. Where are the network bottlenecks?
3. Is the network robust to complicated conditions?
4. What factors affect voice traffic processing?
5. What would be the major load factors?
6. What would be the optimal settings of network parameters?

As previously stated, the topic of convergence needs to be addressed. That is because instead of paying for a separate voice network and a separate data network, everyone nowadays aims at combining the two and run all traffics over one.

NOTE:	For proper convergence to take place, the overall network environment must be equipped with the intelligence necessary for providing translation between different signal types and multipoint routing for establishing connectivity between the different endpoints. There must also be the capability of dynamically reallocating required bandwidth to fulfill different and often difficult endpoint requirements for each communication session.

Most VoIP implementations face problems related to latency and jitter due to the fact that UDP is deployed. A jitter buffer may be put in place to alleviate the problem. Do keep in mind, routing VoIP traffic in the presence of firewalls and address translating proxies may require the use of Private Session Border Controllers along side the firewalls.

NOTE:	Jitter buffers may be used to counter jitter introduced by the packet network. The maximum jitter that may be countered through this buffer equals the buffering delay introduced prior to the start of the play-out of the voice stream.

Fixed delays are quite difficult to control but a little bit of delays can be minimized through marking voice packets as delay sensitive traffic provided that QoS mechanism is in place. On the other hand, since the primary cause of packet losses is congestion, congestion management and avoidance can be helpful.

Echo can be the result of impedance mismatches in the analog circuitry, as well as acoustic coupling of signal at the receiving end.

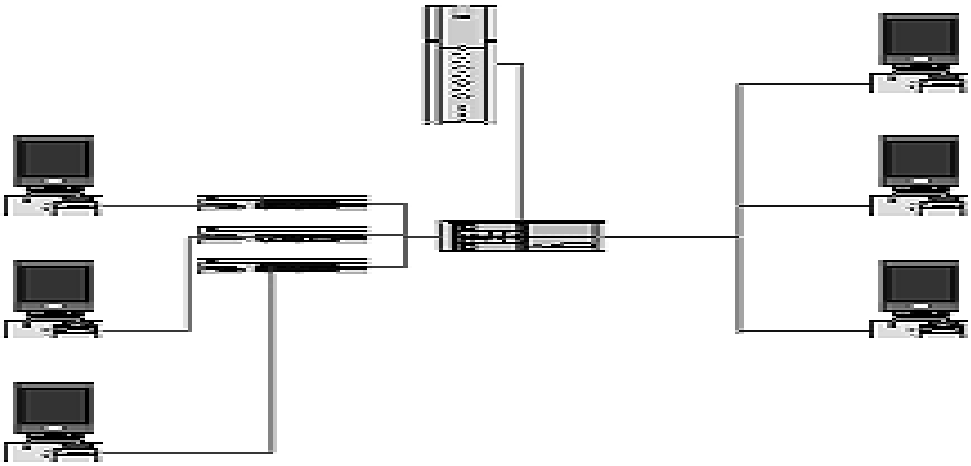
NOTE: According to the ITU-T G.114 specifications, the recommended tolerable one-way delay for voice is 150 ms. In a private network, 200 ms is still acceptable, and anything over 250 ms should not be tolerated.

Both the recommendations of P.800 (MOS) and P.861 (PSQM) are for measuring voice quality. P.800 addresses the use of a method for deriving "a Mean Opinion Score of voice quality". A MOS score can range from 1 (the worst) to 5 (the best). A score of 4 is considered toll quality grade. P.861 attempts to automate the measurement process via a special algorithm. These measurement methods are not without drawbacks, and new methods are constantly in development.

Interpret network diagrams.

As a highly important type of network documentation, use a network diagram to capture all the important information, including and not limited to the topology of a network, the various network device types, the assigned network addresses, the names of switches, routers and other important devices, the physical location of the various hosts, etc…

There are different types of network tools for drawing diagrams. The CCNA exam does require the drawing of these diagrams. However, the exam does require knowing how to read basic diagrams and pick the correct answers that describe the diagrams. An example is shown below for reference:



In particular know the correct locations of routers and the proper “gateway address” settings, as well as the correct host assignment for IP addresses. In other words, know IP V4 subnetting inside and out.

Determine the path between two hosts across a network.

Routing involves the basic activities of determining optimal routing paths and transporting information packets through the network. Routing protocols use metrics for evaluating the best path for a packet to travel. As a standard of measurement, path bandwidth is one commonly used metric used by routing algorithms to determine the optimal path to a destination.

Along the process of path determination, routing algorithms initialize and maintain routing tables. These routing tables are filled with a variety of information, such as destination/next hop and the desirability of paths. Routers compare metrics to determine optimal routes, and keep in mind that the metrics in use can differ a lot depending on the design of the routing algorithm used. Below shows a list of the most popular metrics:

- Path length
- Reliability
- Delay
- Bandwidth
- Load
- Communication cost

The key differentiators of routing algorithms include:

- Static versus dynamic
- Single-path versus multipath
- Flat versus hierarchical
- Host-intelligent versus router-intelligent
- Intradomain versus interdomain
- Link-state versus distance vector

Among these differentiators, pay particular attention to the last one, which is "Link-state versus distance vector".

To enable dynamic routing between Cisco routers, it is necessary to deploy at least one of the following routing protocols:

- Routing Information Protocol (RIP)
- Interior Gateway Routing Protocol (IGRP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)

These protocols can be classified as either distance vector based or link state based. Link-state algorithms flood routing information to all nodes in the network. Each router, however, only

sends out the portion of the routing table that describes the state of its own links. Through this update process, each router can build up a picture of the entire network in its routing tables.

Distance vector algorithms, on the other hand, call for each router to send all or some portion of its routing table only to its neighbors, not to all routers. Therefore, routers that use Distance vector algorithms can only know about their neighbors.

Due to the ability to converge more quickly, link-state algorithms are somewhat less prone to routing loops and are more scalable than their distance vector counterparts. However, link-state based routers require more CPU power than distance vector algorithms, meaning they can be relatively costly to setup and maintain.

If operating on a smaller network and wishing to avoid complicated setup and maintenance tasks, by all means go for the simpler distance vector option. On the other hand, if planning to expand the network shortly and complexity is an option, link-state protocol is the ideal choice.

Describe the components required for network and Internet communications.

A computer network is a system for communication between individual computers. These networks may be fixed via cabling or temporary via modems or other remote connection methods. In fact, computer networks may be categorized based on the following elements and factors:

By scale:

- Local area network (LAN)
- Metropolitan area network (MAN)
- Wide area network (WAN)

By functional relationship:

- Server based
- Peer to peer

By network topology:

- Bus network
- Star network
- Ring network
- Mesh network
- Starbus network

Computer networks can be implemented by using a variety of protocol stack architectures, computer buses or combinations of media and protocol layers. All these are covered in the subsequent exam objectives.

Network Components

A network consists of multiple computers that are linked in order to communicate and share resources. The computers on a network may be linked through different means and are often being referred to as host or network nodes.

When connecting a host, the interface hardware is referred to as a network interface or an adaptor. Networking adapters are also commonly referred to as NICS. These NICs break the computer information into FRAMES or PACKETS for transmission.

Cabling

There are three major types of network wiring, which are Coaxial, Twisted-Pair and Fiber. Each of these cabling types has different requirements for meeting certain network standards.

Following the IEEE 802.3 Standard, coaxial cable is used for 10BASE2 (thinnet) and 10BASE5 (thicknet) networking via a LINEAR BUS topology.

As the next step up from Coaxial, Unshielded Twisted Pair (UTP) cabling uses cable that is made up of four pairs of insulated copper wires. UTP uses RJ45 connectors on each end of the cable for connecting to the network patch panel.

Optical fiber transmits data using pulses of light and can carry data at a rate as high as 622 megabits per second. The good thing about Fiber is that it is not affected by electro-magnetic interference and is very light-weight compared to the copper-based cable. However, it is very costly to install and manage and is therefore not as popular as UTP cabling.

Software

For the network nodes to communicate, their operating systems must be able to speak the same language (which is the network protocol). TCP/IP is the most popular network protocol nowadays and is supported by almost all operating systems currently in the market. Other less popular protocols include the Novell IPX/SPX and the Apple AppleTalk. IOS and the majority of Cisco routers support all of these protocols.

Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach.

A bottom up approach requires that starting at the physical layer. Possible problems at the physical layer can include:

- Incorrect configuration
- Faulty/misconnected cable
- Faulty wiring closet cross-connect
- Faulty interface or port
- Overloaded interface

Do note that based on an official Cisco technical document: *"...it may seem logical to first troubleshoot at the physical layer, problems can generally be found more quickly by first troubleshooting at Layer 3 and then working backward when a physical problem is found or suspected".*

Even though there may be connectivity between a source and a destination, problems may still exist for a specific upper-layer protocol such as HTTP, FTP or Telnet. These protocols are often subject to protocol-specific problems of different kinds. Before troubleshooting at the application level, first establish whether proper connectivity exists between the source and the destination and whether IP is correctly functioning. If IP connectivity is firmly established, then the issue must be at the application layer.

The **PING** command is a very popular method for troubleshooting the accessibility of network devices running in an IP-based environment. It works both in the user EXEC mode and the privileged EXEC mode. By using ICMP echo requests and ICMP echo replies to determine whether a remote network device is up and running, it can at the same time measure the amount of time it takes to receive the echo reply for revealing network performance. In fact, both an ICMP time exceeded message and an ICMP unreachable message may indicate the existence of routing loop, which may occur when there are alternate routes between hosts.

The **extended PING** is used to perform a more advanced check of network device connectivity. It works under the privileged EXEC mode only and offers many more advanced options than the standard **PING** command.

If unable to ping from a router to either the source or the destination, check the routing table on the router for a route to the ping target and find out why the route is missing. If ping succeeds only a percentage of the time, chance is that there may be multiple paths to the destination and that one path may be failing while the others are working. This can be symptomatic of a routing loop (or a physical problem somewhere along the path) and requires that going to all the next hops and test connectivity from there. **PING** and **extended PING** are primarily used in conducting such kind of testing.

Where **PING** can be used to verify connectivity between network devices, the **TRACEROUTE** command can help discover the paths packets take to a remote destination and determine if routing breaks down at a particular point. This is done by recording the source of each ICMP "time exceeded" message along the paths.

As a variation of the standard **TRACEROUTE** command, the **extended TRACEROUTE** command can be used to find out what path packets are taking to get to a destination. The command can also be used to check routing at the same time, which is extremely helpful for troubleshooting routing loops and determining where packets are getting lost.

In a typical troubleshooting scenario, first use the **extended PING** command to determine the type of connectivity problem, and then use the **extended TRACEROUTE** command to narrow down attention to where the actual problem is occurring.

Differentiate between LAN/WAN operation and features.

The Internet consists of a large number of interconnected autonomous systems that are known as ASs. Each of these ASs constitutes a distinct routing domain run by a single organization. Within an AS, all routers communicate with each other using interior gateway protocols. Outside of the organization, ASs are connected via gateways, and the gateway routers are exchanging information using exterior gateway protocols. Routers used for information exchange within ASs are called interior routers, and routers that move information between ASs are called exterior routers.

In any case, for routing to be successful, a proper IP addressing scheme must be made ready. An IP address is the unique number ID assigned to one host or interface in a network. It is 32 bit based. A subnet is a portion of a network sharing a particular subnet address. A subnet mask is a 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host.

Generally speaking, a switch has no knowledge on and does not care about layer 3 addressing information such as IP addresses, so it is kind of “isolated” from those outside hackers on the internet. There are exceptions though. For example, the Catalyst switch itself uses IP address information to communicate with the local routers! Relevant IP information may include the switch IP address, the subnet mask and the default gateway address, which is the address of the router (if any).

Chapter 2 - Implement a Small Switched Network

Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts.

Network Medium

A critical part of designing a LAN is selecting the appropriate network medium. For Ethernet there are several major types of media in use, including Thicknet (for 10BASE5 networks), thin coax (for 10BASE2 networks), unshielded twisted pair (for 10BASE-T networks) and (fiber optic for 10BASE-FL or Fiber-Optic Inter-Repeater Link networks). Among them, the most popular are 10BASE-T and 100BASE-TX, which use unshielded twisted pair cable, which is quite similar to telephone cable.

UTP

Unshielded twisted pair (UTP) cable comes in a variety of grades, with each higher grade offering higher level performance. Level 5 cable is the highest grade which is capable of offering support for transmission rates of up to 100 Mbps. Level 4 and level 3 cable are less expensive but can only support much slower transmissions. Level 2 and level 1 cables are not used in the design of 10BASE-T networks at all.

Fiber Optic

Fiber-optic cable is way more expensive but is invaluable for situations where electronic emissions are a concern or when physical distance exceeds the specifications of the regular UTP cables. Since Fiber-optic cable does not conduct electricity, it is not under the influence of electromagnetic interference. And since the Ethernet standard allows for fiber-optic cable segments up to 2km long, intra-building connection becomes easily implement-able.

Network Type	Max # of Nodes Per Segment	Max Distance Per Segment
10BASE-T	2	100m
10BASE2	30	185m
10BASE5	100	500m
10BASE-FL	2	2000m

Wireless

Wireless LAN is a type of local-area network that uses high-frequency radio waves to communicate between nodes. There is no need for cabling between client nodes. Instead, Access Points are being used to act as the communication hubs for the wireless clients to connect to a wired LAN.

Explain the technology and media access control method for Ethernet technologies.

Ethernet

Ethernet is a LAN architecture developed by Xerox, DEC and Intel way back in 1976. The original implementation uses a bus/star topology and supports data transfer rates of 10 Mbps and serves as the basis for the IEEE 802.3 standard. Below are the key features of Ethernet:

- Every Ethernet frame contains the destination address, source address, type field, and data.
- An Ethernet address is 6 bytes.
- Every network device has its own unique Ethernet address preset in the factory.
- Every network device listens for Ethernet frames with a wild card destination address of "FF-FF-FF-FF-FF-FF", which is a broadcast address.

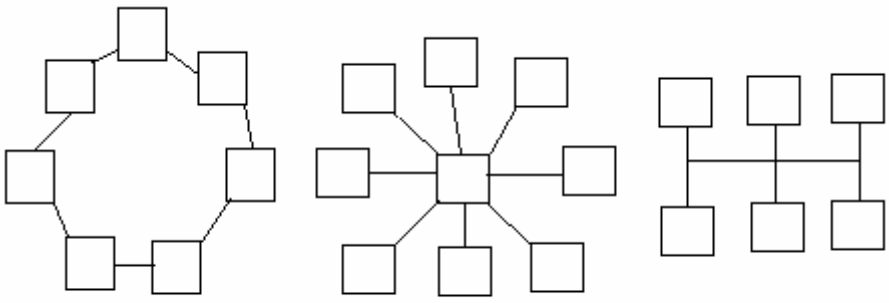
As one of the most widely implemented LAN standards, Ethernet uses CSMA/CD as the access method for handling simultaneous demands. A newer version of Ethernet (known as 100Base-T Fast Ethernet) supports data transfer rates of up to 100 Mbps. Gigabit Ethernet runs even faster - it can go up to 1 gigabit per second in throughput via four pairs of Category 5 UTP cable.

Topology

A network topology refers to the geometric arrangement of nodes and cable links in a LAN. The two popular configurations are bus and star. A typical bus topology consists of nodes linked together in a series with each node connected to a long cable (the bus). Many nodes can tap into the bus and begin communication on that cable segment, but a break anywhere along the bus will cause the entire segment to suffer. 10BASE2 and 10BASE5 networks are based on the bus topology.

The more popular 10BASE-T/100BASE-T Ethernet networks use a star topology in which access is controlled by a central device known as a hub or a LAN switch. One major advantage of a star network is reliability - breakage in one segment will not affect the others.

With a ring topology, nodes are connected from one to another as in a ring. A data token is used to grant permission for each node to send message out. Due to the high cost involved in setting up and maintaining ring networks, they are scarcely found in modern operation these days.



Ring Star Bus

Collision Detection

Ethernet uses Carrier Sense and Multiple Access with Collision Detection (CSMA/CD) for the purpose of collision detection. With all devices communicating on a single medium, only one can transmit at a time (they do, however, all receive the call simultaneously).

CSMA/CD

With CSMA/CD as the access method used in Ethernet, when a host needs to gain access to the network it has to first check and see if the network is free. If the network is free, it goes ahead and sends the signal. If not, it waits a random amount of time before retrying. If the network is free but two devices access the line at exactly the same time, collision occurs. When such collision is detected, they both back off and wait a random amount of time before retrying.

Explain network segmentation and basic traffic management concepts.

Network Segmentation

One way to enhance the efficient of a network is to have it properly segmented. By restricting broadcast traffic to a small local segment wasting bandwidth is avoided, and network scalability is improved for broadcast-intensive protocols and applications that work by flooding out packets everywhere. In fact, there are MANY advantages of network segmentation. They include and possibly not limited to the following:

1. When the maximum physical limitations of a network have been reached, routers may be added to it to create new segments and allow additional hosts to join in.

2. Segmenting the network can reduce the number of hosts per network and therefore reduce the frequency of collision.

3. Dividing a big network into multiple smaller segments can reduce the overflow of problems from one segment to the next.

4. Utilizing segments can ensure that the internal structure of the network will not become visible from the outside world, thus making the network more secure.

LAN Segmentation Using Routers

Segments can be interconnected by routers to enable communication between LANs while blocking other types of traffic. Routers may also be used to allow for the interconnection of disparate LAN and WAN technologies while implementing security mechanisms such as broadcast filters and logical firewalls.

LAN Segmentation Using Switches

Switches work at the data link layer to enable multiple physical LAN segments to be interconnected into a single larger network. Unlike routers, which make decisions based on the layer 3 IP addresses, switches forward and flood traffic based on the layer 2 MAC addresses. LAN switches may be used to segment networks into logically defined virtual workgroups known as VLANs to enjoy substantial benefits in LAN administration, security, and management of network broadcast across the entire network.

VLAN

Virtual LAN (VLANs) refers to a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on different LAN segments. As VLANs are based on logical connections, they are extremely flexible in terms of configuration and application.

Formally speaking, a VLAN is a switched network that is logically segmented on an organizational basis, typically by functions, project teams, or applications. It allows logical network topologies to overlay the physical switched infrastructure such that any arbitrary collection of LAN ports can be combined into an autonomous user group or community of interest. From a technical perspective, a VLAN can be thought of as a broadcast domain that exists within a defined set of switches. Such a broadcast domain can include a number of end systems that are connected by a single bridging domain supported on LAN switches that operate bridging protocols.

VLAN Trunk Protocol (VTP) can greatly reduce administration overhead in a switched network. When configuring a new VLAN on a VTP server, the VLAN is distributed through all switches in the domain, thus reducing the need to configure the same VLAN everywhere. VTP is Cisco-proprietary and is available on most of the Cisco Catalyst Family products.

Explain the operation of Cisco switches and basic switching concepts.

As mentioned previously, routing occurs at layer 3 while switching runs at layer 2. Switches are data link layer devices that enable multiple physical LAN segments to be interconnected. Since switching is performed in hardware rather than in software, it is significantly faster than, say, routing. Most switches use either a store-and-forward switching mechanism or a cut-through switching mechanism when forwarding traffic.

Note that certain Catalyst switches can now perform switching at layer 3 and up.

LAN switching technology employs micro-segmentation for further segmenting the LAN ultimately to a single user with a dedicated LAN segment. Each switch port provides a dedicated full speed Ethernet segment. A LAN switch can enable communication between LANs while blocking other types of traffic. It has the intelligence of monitoring traffic and compiling address tables so that traffic can be forwarded to the specific ports. If necessary it can be configured to provide non-blocking service so that multiple conversations can occur simultaneously. Superior throughput performance, higher port density, lower per-port cost, and greater flexibility are the advantages offered by LAN switches over bridges and hubs.

Perform, save and verify initial switch configuration tasks including remote access management.

Many of the Catalyst switches are designed for plug-and-play operation, meaning all that needs to be done is assigning basic IP information to the switch and connect it to the other devices in the network. The table below shows the typical default settings of the Catalyst switch:

Feature	Default Settings
Administrative connection	Normal mode
Global switch information	No default value for system name, system contact, and location
System clock	No value for system clock time
Passwords	No passwords are configured for normal mode or enable mode.
Switch prompt	Switch>
Interfaces	Enabled, with speed and flow control auto-negotiated, and without IP addresses

If there are network needs, it is possible to perform configuration on an individual basis through the various management interfaces. In particular, individual switches can be configured by using the following interfaces:

- CMS (CiscoWorks management suite), which is a graphical user interface that can be launched from anywhere within the network through a web browser.

- CLI (command line interface), which is the command line that can be accessed by connecting the management station directly to the switch console port or via Telnet from a remote management station. The focus of the exam is in the CLI (which is IOS).

- SNMP (Simple Network Management Protocol), which is supported by SNMP management applications such as the CiscoWorks LAN Management Suite.

IOS stands for Cisco Internetwork Operating System. Cisco describes IOS as a network infrastructure software that integrates a broad range of Internet and enterprise network hardware. From the perspective of a CCNA, however, focus is on the absolute basics - using IOS as the operating system for managing a Cisco router or switch.

Console Port Settings

Rather than performing configuration through the network, a Catalyst switch can be configured locally via the console port.

The switch console port provides switch access to a directly attached terminal or PC through a serial connection and a modem. Ensure that the switch console port settings match the settings of the terminal or PC. The default settings of the switch console port are:

- Baud rate - 9600
- Data bits - 8
- Stop bits - 1
- Parity settings - None

NOTE: In the earlier day where CatOS (the Catalyst OS) has not yet been fully and transparently integrated…

- The default operation of IOS is as a router although it can also be configured to operate as a switch.
- The default operation of CatOS is as a switch, although the switch running Hybrid OS can be configured to operate as a router.
- A hybrid model operates based on two operating images, two configurations, and two command lines (one for CatOS and one for IOS).

Verify network status and switch operation using basic utilities (including: ping, traceroute, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands.

ICMP

PING works using ICMP. Short for Internet Control Message Protocol, ICMP is defined in RFC 792 as an extension to IP. It is a layer 3 (network-layer) protocol that provides message packets to report errors and other information regarding IP packet processing back to the source.

ICMP Messages

ICMP generates several kinds of messages useful for troubleshooting network problems. They are:

- Destination Unreachable
- Echo Request
- Echo Reply
- Redirect
- Time Exceeded

When a destination-unreachable message is sent out by a router, it means that the router is unable to send the package to its final destination. The router then discards the original packet. The four possible types of destination-unreachable messages are network unreachable, host unreachable, protocol unreachable, and port unreachable.

An echo-request message is generated by the ping command for testing host reachability across the network. Such a message typically indicates that the target host can be successfully reached.

A redirect message is sent out by the router to the source host to request for more efficient routing (the router still forwards the original packet to the destination, but just that it wants the sender to choose a better path).

A Time-exceeded message is sent out by the router if an IP packet's Time-to-Live field (which is usually expressed in hops or seconds) reaches zero. This field prevents packets from continuously circulating the network if the network contains a routing loop. The original packet is then discarded.

Note that if an ICMP message cannot be successfully delivered, it will NOT be resent. This is for avoiding an endless flood of ICMP messages.

The SHOW Commands

PING, TRACEROUTE and their variants have been introduced previously. Now we will focus on the use of the various SHOW commands for network troubleshooting. Some of these commands may be executed on a router, while some may also be used on a switch, depending on the network configuration and the kind of troubleshooting being performed.

The show interfaces command can be used to display statistics for all interfaces configured. The resulting output varies depending on the network for which an interface has been configured.

Below is a portion of the sample output from the show interfaces command:

Router# show interfaces

```
Ethernet 0 is up, line protocol is up
  Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
  Internet address is 131.108.28.8, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:00, output 0:00:00, output hang never
  Last clearing of "show interface" counters 0:00:00
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 2000 bits/sec, 4 packets/sec
     1127576 packets input, 447251251 bytes, 0 no buffer
     Received 354125 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     5332142 packets output, 496316039 bytes, 0 underruns
     0 output errors, 432 collisions, 0 interface resets, 0 restarts
---More---
```

Use SHOW IP PROTOCOLS to display the parameters and current state of the active routing protocol process. The information displayed can be very useful in debugging routing operations. In particular, information in the Routing Information Sources field of the output can help to identify a router suspected of delivering bad routing information.

Use SHOW IP ROUTE to display the current state of the routing table. If specifying that the want for information about a specific network displayed (by specifying an address after the command, such as show ip route 10.0.0.1), more detailed statistics can be obtained.

Telnet, SSH, ARP

A virtual terminal (vty) can be accessed through Telnet. A Cisco router can be accessed through vty after it has gone through initial installation. The five virtual terminals available are vty0,vty1,vty2,vty3, and vty4. SSH Terminal-Line Access replaces reverse Telnet with a more secure "secure shell".

ARP establishes correspondences between IP addresses and LAN hardware addresses. A record of each correspondence is kept temporarily in the router cache. To reveal the content of this cache, use the SHOW IP ARP command. If wishing to discover the correspondences between all network addresses (including non-IP addresses) and the LAN hardware addresses, use the SHOW ARP command instead.

Implement and verify basic security for a switch (port security, deactivate ports.)

Port security could be the best tool against spoofing attacks. The port security feature of a Catalyst switch can restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. When secure MAC addresses are assigned to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. On the other hand, if a single secure MAC address is assigned, the workstation attached to that port is assured the full bandwidth of the port.

On a port that is configured as a secure port, when the maximum number of secure MAC addresses is reached and when the MAC address of a workstation attempting to access that port is different from the identified secure MAC addresses, a security violation occurs. Configure the interface to take actions against any of these violations. The available options are primarily Restrict and Shutdown.

Broadcast suppression may also be of great use against attacks that aim at flooding the network. This feature refers to the use of filtering techniques to measures broadcast activity in a subnet over a one-second interval and compares the measurement with a predefined threshold. If the threshold is reached, further broadcast activity is suppressed for the duration of the interval.

Identify, prescribe, and resolve common switched network media issues, configuration issues, autonegotiation, and switch hardware failures.

The show commands can also be used to monitor switch behavior during initial installation; to monitor normal network operation; to isolate problem interfaces, nodes, media, or applications; to determine when a network is congested; and to determine the status of servers, clients, or other neighbors.

The debug commands may be used to provide a wealth of information about the traffic on an interface, error messages generated by nodes on the network, protocol-specific diagnostic packets and cells, and other useful troubleshooting data.

NOTE:	Many debug commands are processor intensive and can cause serious network problems if they are running on an already heavily loaded switch.

Keep in mind; when troubleshooting a network environment, the recommended approach is to first define the specific symptoms, then identify all potential problems that could be causing the symptoms, and systematically eliminate each potential problem until the symptoms disappear.

NOTE: There is a 7-step method that is recommended by Cisco. The steps are:

1. Analyze the network problem and create a statement of the problem.
2. Gather the facts to help isolate possible causes.
3. Consider possible causes and eliminate potential problems from the list.
4. Create an action plan based on the remaining potential causes.
5. Implement the action plan.
6. Analyze the results to determine if the problem has been resolved.
7. If the problem has not been resolved, return to Step 4 and repeat the process.

In summary,

- A layer 1 problem means a physical connectivity problem.
- A layer 2 problem usually means a problem associated with LAN switching.
- A layer 3 problem usually means a problem associated with IP addressing or routing.
- A layer 4 or above problems are likely related to the applications.

If the switch port statistics show loads of alignment errors or frame check sequence, there may be speed or duplex mismatch between both end device ports (probably due to autonegotiation error). Manually inspecting and changing these settings accordingly may be necessary.

If the problem is believed to be on the network media, the following tools may prove useful:

- Use Volt-ohm meters and digital multimeters to measure physical layer parameters such as AC and DC voltage, current, resistance, capacitance, and cable continuity.
- Cable testers can test and report on cable conditions such as near-end crosstalk, attenuation, and noise; perform time domain reflectometer functions, traffic monitoring, and wire map functions; and display MAC-layer information about LAN traffic as well as provide statistics on network utilization and packet error.
- What condition are the cables in? Do they appear damaged?

Standard	Media Type	Cable Length	Transfer Speed	Connector
10BaseT	Cat3 or higher UTP	100 meters	10 Mbps	RJ45
100BaseTX	Cat5 or higher UTP	100 meters	10 Mbps	RJ45
100BaseFX	Fiber optic	100 meters	10 Mbps	Fiber optic
1000BaseT	Cat5 or higher UTP	100 meters	10 Mbps	RJ45
1000BaseSX	Fiber optic	100 meters	10 Mbps	Fiber optic
1000BaseLX	Fiber optic	100 meters	10 Mbps	Fiber optic
1000BaseCX	Fiber optic	100 meters	10 Mbps	Fiber optic

Keep in mind, 10BaseT and 100BaseTX cable cannot exceed 100m in length.

A network may be kept trouble-free by running a proactive maintenance plan regularly. A comprehensive network maintenance plan shall comprise of checks on key network devices such as switches, hubs, routers, print servers, printers, firewall, and even UPS.

In particular, the network can be kept smooth and reliable by regularly running a proactive maintenance plan on infrastructure items, such as the horizontal wiring that extends from the wall outlet to the central closet, which should normally include the wall outlet, the horizontal cable and any cross-connects or patch cables. Normally the patch cords as well as the cross-connect leads have a length limit of 6M. There should be outlets for phone and data, and that standardized media should be deployed. Also take good care of the backbone wiring system, which is useful for interconnecting telecommunication closets and equipment rooms/entrance facilities.

NOTE:

A link LED on a switch cannot guarantee that the connected cable is fully functional. Always verify the connection by pinging from the directly connected switch.

Keep in mind, for connections involving 10BASE-T, 100BASE-TX, and 1000BASE-T, the max distance between the port and the attached devices cannot exceed 100 meters.

The switch's front-panel LEDs provide basic troubleshooting information about the switch hardware by showing power-on self-test failures as well as port connectivity problems and switch performance issues.

NOTE:	POST tests shall run automatically every time the switch is turned on. The show POST command can be used to find out if any of the POST tests has failed.

For a very serious problem with the device

show tech-support outputs the equivalent of the show version, show running-config, show controllers, show stacks, show interfaces, show buffers, show process memory, and show process commands. Sometimes it might be useful to obtain a core dump and turn it over to the Cisco technical support representative for further troubleshooting. However, it is necessary to realize that creating a core dump while the switch is running can seriously disrupt the current network operation.

Chapter 3 - Implement an IP Addressing Scheme and IP Services to Meet Network Requirements for a Small Branch Office

Describe the need and role of addressing in a network " Create and apply an addressing scheme to a network. Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment.

In terms of IP addressing, it is very important to consider the scalability requirement. Is the current way of subnetting sufficient for accommodating additional new users in the coming days? Is Ipv4 all that is being implemented or will IPv6 be implemented also?

In order to properly communicate on an internetwork, computers must have unique identifiers for differentiating one computer from another. This is accomplished through IP addressing. Every IP V4 address is made up of a 32-bit address or 4 "octet" address. Each bit in the octet has a binary weight of 128, 64, 32, 16, 8, 4, 2 or 1, with a minimum numeric value of 0 or a maximum value of 255. The address is written using decimal numbers separated by decimal points, which is commonly being referred to as the dotted decimal notation of expressing IP addresses. For example: 192.78.213.5.

An IP Network is identified by the number of bits in the network mask. On the other hand, the node addresses are arbitrary numbers that are mapped to the physical addresses of the network hosts within the IP network. The basic rule of thumb is that every network host has at least one unique IP address, while every router has a unique IP address for every network interface it possesses. All hosts on the same physical network must have the same network prefix in order to communicate with each other.

NOTE:

IP addresses are grouped into different classes. These so called “Classes” are allocated to organizations that request them in address blocks. INTERNIC is the organization that administers and assigns the IPV4 classes and addresses.

Class A addresses range from 1.X.X.X to 126.X.X.X, where the first octet identifies the network (the prefix) and the last three octets identify the node. The default subnet mask is 255.0.0.0:

11111111.	00000000	00000000	00000000
Network	node	node	node

Class B Addresses range from 128.0.0.X to 191.255.X.X, where the first two octets identify the network and the last two identify the node. The default subnet mask is 255.255.0.0:

11111111.	11111111	00000000	00000000
Network	Network	node	node

Class C Addresses range from 192.0.0.X to 223.255.255.X, where the first three octets identify the network and the last octet identifies the node. The default subnet mask is 255.255.255.0:

11111111.	111111111	11111111	00000000
Network	Network	Network	node

The address that starts with 127 is the loopback address that represents the local interface. For example: 127.x.x.x. The contents of the last three bytes are not of any concern. The 127.x.x.x address is typically used for troubleshooting purpose. It verifies that a network host can actually send something to itself, meaning the host’s TCP/IP stack is still functioning (at least on itself).

Addresses from 224.0.0.0 to 239.255.255.255 are used for multicast packets, and this entire address range is known as the Class D address range. The Class E address range is also reserved, for experimental purpose.

IP Address Class	Address Range	Usage	Maximum number of hosts that can be accommodated.
A	1.0.0.0 to 126.0.0.0	For very large organizations	16,777, 214[2] (2^{24} - 2)
B	128.1.0.0 to 191.254.0.0	For med size organizations	65, 543 (2^{16} - 2)
C	192.0.1.0 to 223.255.254.0	For smaller organizations	245 (2^{8} - 2)
D	224.0.0.0 to 239.255.255.255	N/A	N/A
E	240.0.0.0 to 254.255.255.255	N/A	N/A

Note that the system of IP address classes that have just been described is generally bypassed today by the use of Classless Inter-Domain Routing (CIDR) addressing.

With CIDR, each address has a network prefix for identifying either an aggregation of network gateways or an individual gateway. The length of such prefix is also specified as part of the address and can vary greatly depending on the number of bits that are actually needed. A destination address that has a shorter prefix is said to be less specific. A longer prefix, on the other hand, is said to describe a destination gateway more specifically. When routing, routers are required to use the more specific prefix in the routing table when forwarding packets.

A classless network address should look something like 192.22.25.00/18, where "18" says that the first 18 bits of the address represent the network and the last 14 bits represent the specific host addresses.

The IPv6 address space has 128 bits, which is broken down into eight groups of 16 bits. There are two major 64-bit parts, which are the network prefix (contains the registry, provider, subscriber ID, and subnet) that occupies the higher order groups of bits and the interface ID that occupies the lower bits.

The three major types of IPv6 addresses are unicast, anycast, and multicast. An IPv4-mapped IPv6 address may be used to identify an IPv4-only node to an IPv6 node. For purpose of the exam, it is not required to drill into IPv6 implementation.

Explain the basic uses and operation of NAT in a small network connecting to one ISP.

Network Address Translation (NAT) allows a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. It helps securing a network by masking the internal configuration of a private network and makes it difficult for outsider to monitor individual users.

With Dynamic NAT, a private IP address is mapped to a public IP address drawing from a pool of public IP addresses. On the other hand, Static NAT is recommended only for small user base.

In any case, the first step in NAT deployment is to define NAT inside and outside interfaces. With dynamic NAT, the translation table in the router is initially empty but will get populated once traffic passes through the router.

NOTE: IMPORTANT: The NAT function should be located at the point where the LAN meets the WAN.

NAT is in fact a good security measure as it can hide the internal addressing structure. PAT, on the other hand, uses port remapping so that a single valid IP address may support source IP address translation for up to 64,000 clients. PAT does not work with applications that have an inbound data stream different from the outgoing control path. Another option would be to use Static translation, which allows for the substitution of a fixed external IP address for an internal address, which is useful for servers that require fixed IP addresses.

Describe and verify DNS operation.

With DNS, mapping between host names and IP addresses is created. One easy way to verify whether DNS is working is to use operating system utility such as Nslookup at the command prompt to display information that diagnoses DNS infrastructure. Do keep in mind, this is a text mode utility and is available only if the TCP/IP protocol is installed on the computer.

```
C:\>nslookup www.examreview.net
Server:
Address:  192.168.2.1

Name:    www.examreview.net
Address:  75.126.94.74
```

There has to be a functioning DNS server on the network. Mapping is usually a dynamic process, although certain DNS server software allows mapping entries to be created statically.

Describe the operation and benefits of using private and public IP addressing.

Private IP addresses belong to the address space allocated via RFC 1918. These addresses are available for any use by anyone such that the same RFC 1918 IP addresses can be reused anywhere without introducing conflicts. However, because these addresses are not routable, they must stay "private" without connecting to the Internet. In fact, for hosts configured with private addresses to access the internet, the Network address translation (NAT) function would be desired.

The formally defined private network address spaces are:

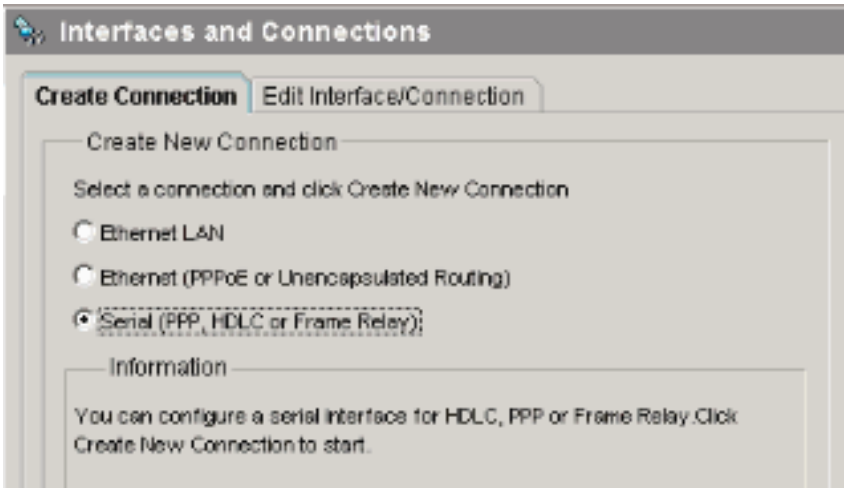
Name	IP address range	Number of IPs
24-bit block	10.0.0.0 – 10.255.255.255	16,777,215
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576
16-bit block	192.168.0.0 – 192.168.255.255	65,535

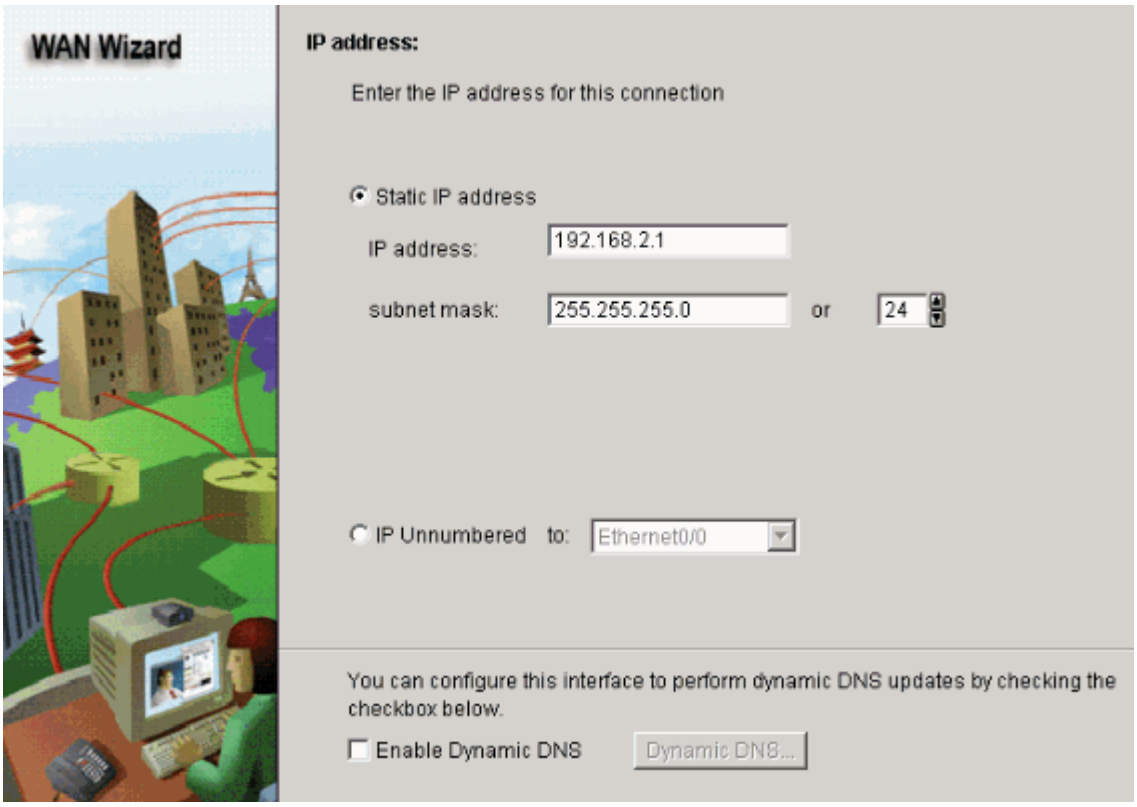
In fact, operating systems' support for APIPA (Automatic Private IP Addressing) makes it unnecessary to worry about private address configuration. With APIPA, the local DHCP clients can automatically self-configure an IP address and subnet mask when a DHCP server is not online. The available IP address range is 169.254.0.1 through 169.254.255.254 on the most popular Microsoft OS platforms.

NOTE: With private addressing, it is not required to pay to use IP addresses. There is total freedom on address assignment, and there are plenty of free addresses to use. With public addressing, addresses are paid for through the service provider, and rules have to be followed in assigning addresses. The best thing to do would be to use private addressing inside the internal network, and through NAT the public addresses may be used for outgoing access.

Enable NAT for a small network with a single ISP and connection using SDM and verify operation using CLI and ping.

SDM has a WAN wizard that may be used to configure NAT for outgoing access. The screen captures below are self-explanatory. After configuration, ping may be used to test the connection.





Configure, verify and troubleshoot DHCP and DNS operation on a router (including CLI and SDM.) Implement static and dynamic addressing services for hosts in a LAN environment.

DHCP

DHCP as explained in RFC 2131 is built on a client/server model for providing automatic configuration parameters to Internet hosts. It consists of a protocol for delivering host-specific configuration parameters from a DHCP Server to a host and a mechanism for allocating network addresses to multiple hosts. The three mechanisms for IP address allocation include Automatic allocation (which assigns a permanent IP address to a client), Dynamic allocation (which assigns an IP address to a client for a limited period of time or until the client explicitly relinquishes the address), and Manual allocation (address assignment configured entirely by hand).

Benefits of Dynamic Address Assignment

Dynamic address assignment through DHCP offers the following benefits:

- Reduced Internet access costs – with automatic IP address assignment for each remote site, Internet access costs can be significantly reduced due to the fact that static IP addresses are considerably way more expensive to purchase.

- Reduced client configuration tasks and costs - DHCP is easy to configure and can therefore minimizes operational overhead and costs associated with device address configuration

- Centralized management – a single DHCP Server can maintain configurations for several subnets, thus allowing centralized administration.

How does DHCP work?

The Cisco IOS DHCP Server feature can be used to assign IP addresses from specified address pools within the router to the DHCP clients. When a DHCP client needs to request an IP address from a DHCP Server, it sends a DHCPDISCOVER broadcast message to locate the IOS based DHCP Server. The DHCP Server in return offers configuration parameters such as IP address, MAC address, domain name, and lease time to the client through a DHCPOFFER unicast message.

By default, the IOS based DHCP server feature is enabled on the router. If there is a need to re-enable the feature due to whatever reason, simply enter into global configuration mode and use the command SERVICE DHCP.

To configure a DHCP address pool and enter into the DHCP pool configuration mode, use the IP DHCP POOL command in global configuration mode. The DHCP Server assumes that all IP addresses in its address pool are available for assignment. If there is a need to allow exceptions, manually configure the exclusion of IP addresses.

Automatic bindings refer to IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database. These bindings are stored as text records on a remote host (which is known as a database agent). Manual bindings, on the other hand, refer to IP addresses that have been manually mapped to the MAC addresses of the hosts found in the DHCP database. Unlike automatic bindings, manual bindings are stored in the NVRAM of the DHCP Server.

Identify and correct IP addressing issues.

Subnet Mask Configuration

Most of the time problems occur due to improper address / subnet mask configuration. To begin troubleshooting, display and examine the IP configuration of the host. To do so,

- On a Cisco router, use **show ip interface** and **show running-config** (or it may be better to use the GUI based SDM to do all of the configuration works).
- On Windows 95, 98 or ME, use **winipcfg.**
- On Windows NT, 2000, XP or 2003, use **ipconfig**.
- On UNIX or Linux, use **ifconfig**.

If no IP address is configured, verify that this host receives its IP address from BOOTP or DHCP. Otherwise, an IP address should be manually configured for this interface. On the other hand, if the incorrect IP address, subnet mask, or default gateway is configured, verify that this

host receives its IP address from BOOTP or DHCP, and then request the DHCP or BOOTP administrator to troubleshoot the DHCP or BOOTP server's configuration.

Duplicate IP Address

In order to rule out a duplicate IP address, which is usually caused by incorrect manual configuration by the administrator, first identify a suspect device and have it removed from the network, then try pinging the device from another device on that same network segment. If the ping is successful, another device on that network segment is using the same IP address. The conflicting MAC address can be determined by inspecting the ARP table on the pinging device.

Addressing Considerations

A well-planned IP addressing scheme can provide an organization with important benefits. When planning an IP addressing scheme, try to cover all of the networks currently in use as well as making the best estimation on additional networks and hosts in the foreseeable future.

If the network is to be segmented into smaller sections, it will be necessary to plan the number of subnets to deploy. Routing is an important issue to consider when planning for network segmentation. www need to determine how networks are going to communicate with each other, and what addresses are to be used by the default gateways.

NOTE: Segments can be interconnected by routers to enable communication between LANs while blocking other types of traffic. Routers may also be used to allow for the interconnection of disparate LAN and WAN technologies while implementing security mechanisms such as broadcast filters and logical firewalls.

VLSM

With the traditional way of subnetting, the same subnet mask is applied for all the subnets, meaning each subnet has the same number of available host addresses. In many cases, having the same subnet mask for all subnets can waste address space as each subnet just cannot utilize all the available host addresses.

In order to use IP address space more efficiently, Variable Length Subnet Masks (VLSM) can be deployed. VLSM can allow for the use of a long mask on networks with few hosts and a short mask on subnets with many hosts. This technique is efficient in terms of address space usage, but is considerably more complex. Also keep in mind that in order to use VLSM, A routing protocol that supports it must be used.

Chapter 4 - Implement a Small Routed Network

Describe basic routing concepts (including: packet forwarding, router lookup process.)

Overview of Routing Protocol Characteristics

Routing protocols specify how routers exchange routing table information. Interior gateway protocols are used to exchange routing information among routers in an autonomous network within a confined geographical area. Examples include RIP, RIP V2, OSPF, IGRP and EIGRP.

Exterior routing protocols, on the other hand, are used to exchange routing information between two hosts in a network of autonomous systems that are geographically separated. BGP is an example of exterior routing protocol.

A routing domain or routing realm refers to the collection of routers that exchange routing information. A router redistributes routes when the routes are learnt from a source external to the routing process. The router that redistributes routes from one domain to another is often being referred to as the border router as it borders the differing domains.

Performance Factors

Convergence refers to the time it takes for a router to update its routing tables. Routing protocols that send out the entire routing table typically consume more bandwidth and take longer to complete the update process, and is said to be less scalable.

Periodic broadcasts of the full routing table tend to consume a large amount of bandwidth, which can be a major problem with large networks that run on slow links and WAN clouds.

It is believed that RIP does not perform well in large networks because:

- RIP routers broadcast the entire routing table periodically.
- RIP routers have to go through a period of a hold-down and garbage collection and have to slowly time-out information that has not been received recently.

Also understand that RIP networks are flat networks (due to the absence of concepts such as areas and boundaries), which is why classless routing and route aggregation/summarization do not work under RIP.

OSPF, on the other hand, uses a highly complicated link-state algorithm to build and calculate the shortest path to all known destinations, which allows much faster convergence in large networks. OSPF enables the logical definition of networks where routers can be divided into areas. Therefore, the explosion of link state updates can be limited over the whole network and provide a mechanism for aggregating routes as well as reducing the unnecessary propagation of subnet information. There is a price to pay though – OSPF is complicated to setup and is highly demanding in terms of router processing power.

Describe the operation of Cisco routers (including: router bootup process, POST, router components.)

Router Hardware

As previously mentioned, routing involves the basic activities of determining optimal routing paths and transporting information packets through the network. Routing protocols use metrics for evaluating the best path for a packet to travel.

A router is a computer dedicated to routing functions. Therefore, it has a chassis, a processor, memory, expansion slots (on certain models) and some ports / network interfaces. It also has a power supply for providing power to the various functioning components within it.

Memory Components

The basic internal memory components of a Cisco router include ROM (memory containing micro-code for basic functions to start and maintain the router), DRAM (which stores the running configuration, routing tables, and packet buffers), NVRAM (which stores the system's configuration file and the configuration register), and Flash Memory (which stores the IOS image). Note that Flash memory is either EEPROM based or PCMCIA card based.

DRAM can be logically divided into Main Processor memory (for storing routing tables, fast switching cache, and running configuration) and Shared Input/Output (I/O) memory (for temporary storage of packets in system buffers at the time of switching).

Registers

Registers are the small but fast memory units inside the router for storing special purpose information like interrupt status and instruction currently in execution ... etc. The main processor contains the instruction register, the general purpose registers for integer and floating point data, and other control registers. The UART contains its own status register as well.

Boot-up Sequence

When a typical Cisco Router is first powered up, the boot-up sequence involves the following steps:

1. ROMmon (ROM Monitor) takes control of the Main Processor and handles a number of tasks, including Control register settings, Console settings, Initial diagnostic tests of memory and other hardware, Data structure initialization, and Flash file system setup.

2. Based on the configuration register value stored in the NVRAM, the router either stays in ROMmon or has RxBoot executed from the Boot ROM.

3. RxBoot analyzes the hardware. Then, based on the configuration register value, the router either stays in RxBoot, or the IOS software image file is executed from Flash or from RAM.

4. The main IOS software image analyzes the router hardware again, and then create the data structures necessary for loading the startup configuration.

Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts.

Please refer to Objective 1 of Chapter 2 for information on this topic.

Configure, verify, and troubleshoot RIPv2.

RIP as a distance vector protocol is easy to setup but is limited by hop counts. RIP 2 allows more information to be included in RIP packets and provides a simple authentication mechanism that is not supported by RIP. In fact, the primary difference between RIP V2 and V1 is that RIP V2 supports plain text authentication and MD5 authentication, with plain text authentication being the default. To specify the type of authentication to use, invoke the ip rip authentication mode command.

Also note the following commands:

- To specify the RIP version to receive on an interface basis, invoke the ip rip receive version command.
- To specify the RIP version to send on an interface basis, invoke the ip rip send version command.
- To examine the current state of the RIP routing table, use show ip route. To display information on RIP routing transactions, use the debug ip rip command.

Split Horizon

Generally speaking, routers in a broadcast-type IP network that uses distance-vector routing protocols (such as IGRP and RIP) employ the split horizon mechanism to minimize the likelihood of routing loops. The split horizon mechanism blocks information about routes from being advertised by a router out of any interface from which that information originated. This behavior is supposed to be capable of optimizing communications among multiple routers, especially when links are broken. However, with certain non-broadcast networks this behavior may not be desirable at all. For example, when an interface is configured with secondary IP addresses and split horizon is enabled, updates may not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

In order to enable split horizon, use the ip split-horizon command. To have it disabled, use the no form of this command.

Router Resources

Sometimes a router may appear sluggish or may not respond at all, which is quite likely a hardware resource issue. Here is what to do to check the router's resources:

- To check the available router memory, use the **show memory** command and look at how much memory is available in the **largest free** field. There should be at least 5 percent of total router memory as free. If this is not the case, use **show process memory** to identify the process that is eating up router memory.

- To determine if a router CPU is overloaded, use the show process cpu command. If the level of total CPU utilization is greater than 90% most of the time, something is definitely wrong and **show process cpu** should be used to find out which processes are running and how much CPU they are using.

Access and utilize the router CLI to set basic parameters.

Modes of Router Operation

Before using any of the IOS commands, it is important to understand the difference between the major modes of router operation.

When first turning on a Cisco router, the Setup mode is entered first, which is different from the various configuration modes shown below in that it appears without the presence of any configuration file. Upon entering this mode, some basic configuration parameters may be specified for the Cisco router.

- The User EXEC mode with a prompt of “Router>” represents lowest level of router access. This mode allows for the examination of router status, check routing tables, and perform some basic diagnostics. However, it is not an option to change the router configuration, view the configuration files, or control the router to perform the more sophisticated tasks.

- The Privileged (enable) EXEC mode with a prompt of Router# allows one to have all the privileges of EXEC (user) mode as well as commands that allow one to view configuration files, change the router configuration, and perform complicated troubleshooting tasks. Note that when working in this mode, it is possible to get back to the user mode by entering "disable" at the "#" prompt.

- The Global Configuration mode with a prompt of Router (Config)# allows one to perform tasks that may affect the entire router, including and not limited to naming the router, configuring the banner messages and enabling/disabling the routed protocols.

The ROM monitor mode is a separate mode. It is used when the router cannot boot properly. If the router does not find a valid system image when it is booting, or if its configuration file is corrupted at startup, the system might enter ROM monitor mode.

Connect, configure, and verify operation status of a device interface. Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities.

Interface Configuration

Generally speaking, when configuring interfaces for LAN connections it is only necessary to assign a network layer address and ensure that the corresponding interface is not administratively shutdown. If configuring for WAN connections, however, it is very likely the appropriate data link layer encapsulation will need to be set up. As an example, serial interfaces default to using HDLC. For in-depth information on WAN connections please refer to the last chapter.

The SHOW Commands

In order to analyze network problem, the first thing to do is to check and see if problems exist on the router itself. The SHOW command and its subset are extensively used for verifying the status and configuration information of the Cisco router. Do note that the SHOW command is used in privileged EXEC mode most of the time.

- Use the SHOW RUNNING-CONFIGURATION command to display the router's active configuration file, passwords, system name, as well as interface settings and interfaces IP addresses.
- Rely on the SHOW INTERFACE command to display status and configuration information of the local interfaces.
- Use the SHOW PROCESS command to display the router's CPU utilization.
- Rely on the SHOW CONFIG command to display information on the startup configuration of the router.

NOTE: The set ip route command can be used to add new IP addresses or aliases to the IP routing table. It is also possible to use show ip route to display the current IP routing table entries.

The DEBUG Commands

The DEBUG commands, which are supposed to be entered in privileged EXEC mode, are very useful for troubleshooting problematic network traffics. Output formats do vary with each DEBUG command, and since debugging output is assigned high priority in the CPU process, it is best to use DEBUG commands during periods of lower network usage.

The DEBUG ALL command is used to enable all system diagnostics. It is also possible to use the DEBUG ? command to retrieve a list of brief descriptions on all the debugging command options.

PING, TRACEROUTE, and Their Variations

For information on these commands please refer to Objective 10 of Chapter 1.

Perform and verify routing configuration tasks for a static or default route given specific routing requirements.

RIP

RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. By default, IOS sends routing information updates every 30 seconds. The metric used by RIP to rate the value of different routes is hop count, which is the number of routers that can be traversed in a route. A directly connected network has a metric of zero, while an unreachable network has a metric of 16.

If a router has a default network path, RIP advertises a route that links the router to the pseudonetwork 0.0.0.0. This network does not really exist; it is simply used by RIP to implement the default routing feature.

Use the router rip command to enable a RIP routing process and enter into the router configuration mode.

IGRP

IGRP uses a combination of user-configurable metrics, such as internetwork delay, bandwidth, reliability, and load. It advertises three types of routes, which are interior, system, and exterior. Interior routes are routes between subnets in the network attached to a router interface. System routes are routes to networks within an autonomous system. Exterior routes are routes to networks outside the autonomous system that are considered when identifying a gateway of last resort.

By default, a router running IGRP sends update via broadcast every 90 seconds. It declares a route inaccessible if it does not receive an update from the first router in the route within 270 seconds. After 630 seconds, it removes the route from the routing table entirely.

Use the router igrp command to enable an IGRP routing process and enter into the router configuration mode. Remember to specify the desired autonomous-system with this command.

OSPF

The Cisco implementation of OSPF conforms to the Version 2 specifications detailed in the Internet RFC 2328. It typically requires coordination among many internal routers, such as the area border routers (ABRs - routers connected to multiple areas) and the autonomous system boundary routers (ASBRs). At a minimum, OSPF-based routers can be configured with all default parameter values and with no authentication enabled. However, if intending to customize a network environment, it is imperative to carefully coordinate the configurations of all the running routers.

To enable OSPF in a network, create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range of IP addresses.

The router ospf command is used to enable OSPF routing and enter into the router configuration mode. Remember to supply a process-id for this command. Then use the network address wildcard-mask area area-id command to define an interface on which OSPF runs and the area ID for that interface.

EIGRP

EIGRP has the basic components of Neighbor discovery of neighbor recovery, Reliable transport protocol, DUAL finite state machine and Protocol-dependent modules. Neighbor discovery of neighbor recovery refers to the process that routers use to dynamically learn of other routers on their directly attached networks. The reliable transport protocol is responsible for guaranteed and ordered delivery of EIGRP packets to all neighbors. The DUAL finite state machine embodies the decision process for all route computations. The protocol-dependent modules are responsible for most network layer protocol-specific tasks.

Use the router eigrp command to enable an EIGRP routing process in global configuration mode. Remember to specify an autonomous-system with this command. Then use the network command together with a network-number to associate networks with an EIGRP routing process under the router configuration mode.

Manage IOS configuration files (including: save, edit, upgrade, restore.) Manage Cisco IOS.

User Interface

The Cisco IOS user interface is command line based (known as CLI). The main reason for using a command-line interface instead of a menu driven one is speed. Knowing the commands inside and out helps to perform the tasks much faster, instead of having to browse through menus.

> *Cisco IOS is standard across all Cisco routers.*

System Images

A system image contains a version of the IOS software. A router should already have an image on it when it was delivered. However, it may be beneficial to load a different image onto the router at some point, such as when wanting to upgrade the software to the latest release.

The two main types of images a router may use are the System Image and the Boot Image. The System image contains the complete Cisco IOS software, and is loaded when the router boots. Do note that on most router platforms the System image is located in Flash memory. The Boot image, on the other hand, is a subset of the IOS software. This image is used for network booting or for loading the Cisco IOS images onto the router. This image is also used if the router cannot find a valid system image. Note that on some platforms, the boot image is contained in ROM. In others, the boot image may be stored in Flash memory.

Cisco platforms generally use one of three different Flash memory file system types, which are:

Type	Cisco Platforms
Class A	Cisco 7000 family, Cisco 12000 series routers, LightStream1010 switch
Class B	Cisco 1003, Cisco 1004, Cisco 1005, Cisco 2500 series, Cisco 3600 series, and Cisco 4000 series routers, and Cisco AS5200 access servers
Class C	Cisco MC3810 multiservice

For information on the router's memory components, please refer to Domain 3 – Objective 9.

Transferring Images to Servers

System images can be copied from Flash memory to a server via FTP, rcp, or TFTP. This is done so that a backup copy can be stored on the server for recovery purpose or for verifying that the copy in Flash is the same as the original file on disk. The choice of protocol depends on server availability (which type of server is being used) and the performance/reliability goal (the FTP and rcp transport mechanisms provide faster performance and are in general more reliable than TFTP).

The SHOW FLASH: command can be used to learn the name of the system image file and then the COPY FLASH: FTP: command to copy the system image to a FTP server. Alternately, do not use the COPY FLASH: TFTP: command to copy the system image to a TFTP server, or COPY FLASH: RCP: to copy the system image to a rcp server.

Transferring Images to the Flash Memory

Normal or compressed images can be copied to the router's Flash memory. To produce a compressed system image, from any UNIX platform use the compress interface configuration command. Do ensure that enough space is available before copying a file to Flash memory. The best thing to do is to use the SHOW FLASH-FILESYSTEM: command to examine the flash system and then compare the size of the file to be copied to the amount of Flash memory available. In any case, the commands for performing the copy are easy:

```
COPY FTP: FLASH:
COPY TFTP: FLASH:
COPY RCP: FLASH:
```

Before booting the router from Flash memory, it is suggested that to use the VERIFY command to verify that the checksum of the image in Flash memory matches the checksum listed in the README file that was distributed with the system software image. The checksum of the image can be located in Flash memory at the bottom of the screen when using the COPY command to copy an image.

Initial Configuration

AutoInstall and Setup are facilities that can assist in setting up the initial configuration of a Cisco router.

The AutoInstall facility itself has no unique commands as its functionality is built entirely on other IOS commands. To use AutoInstall, however, *requires preparation* in advance. One way is to create a minimal configuration file that provides just enough configuration information to allow one to Telnet to the new router. The other way is to create a host-specific configuration file for each new router containing all of the necessary configuration information, and then have the configuration file stored on a TFTP server on the network prior to connecting the new router.

The setup command facility, on the other hand, is an interactive facility that allows one to perform first-time configuration and other basic configuration procedures on the router. It works by prompting one to enter basic information needed to get the router started. At the Router# prompt one simply enters the SETUP command, and the screen will display "System Configuration Dialog" together with a series of configuration questions that need to be answered.

Router Configuration Files

Router configuration files contain the Cisco IOS software commands for customizing the functionality of the Cisco router. Commands are parsed by the IOS when the system is booted from the startup-config file or when entering commands at the command line in a configuration mode.

Startup-config refers to the startup configuration files used during system startup to configure the software. Running-config, on the other hand, refers to the running configuration files that contain the current configuration of the software. These two configuration files can be identical or different, depending on what is on them.

Startup Config and Running Config

The contents of the configuration file that will be used at the next system startup can be displayed via the SHOW STARTUP-CONFIG command in Privileged EXEC mode. Such a command can display the contents of NVRAM (if present and valid) or the configuration file pointed to by the CONFIG_FILE environment variable. On the other hand, the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or virtual circuit class can be displayed with the SHOW RUNNING-CONFIG command in privileged EXEC mode.

As the various IOS configuration modes are used, commands generally are executed immediately and are saved to the running configuration file either immediately or when exiting the configuration mode. Do note that IOS accepts only one configuration command per line, although it is possible to enter as many configuration commands as desired.

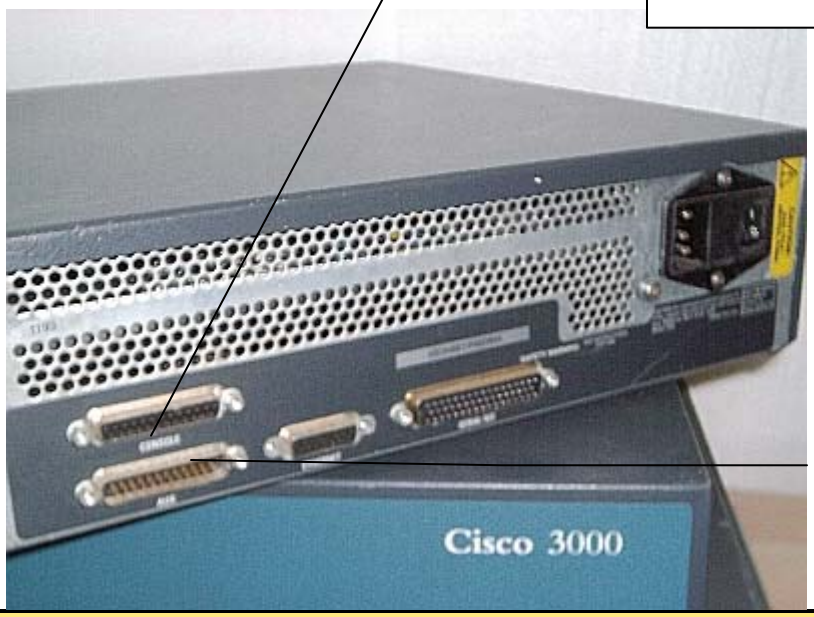
To modify the startup configuration file, either save the running configuration file to the startup configuration using the COPY RUNNING-CONFIG STARTUP-CONFIG command, or copy a configuration file from a file server to the startup configuration.

Compressing Configuration File

With the SERVICE COMPRESS-CONFIG global configuration command, it is possible to specify that the configuration file be stored compressed in NVRAM. A configuration file that is compressed will not prevent the router from functioning normally. In fact, when the router is booted, it will recognize that the configuration file is compressed and will therefore expand and use it as usual.

Implement password and physical security.

As described before the IOS is divided into several different modes, and that the commands available at any given time depend primarily on which one is currently in. When logging in, one begins in the User EXEC mode with only a limited subset of the commands available. To access all other commands, enter the privileged EXEC mode by supplying a password. In fact, IOS supports several different types of passwords. Use the ENABLE PASSWORD command to restrict access to the privileged exec mode through the use of a non-encrypted password. The ENABLE SECRET command is used to assign a one-way encrypted secret password instead of the enable password. A virtual terminal password is used for Telnet sessions into the router. An Auxiliary password is used for restricting access through the auxiliary port. A Console password is used to restrict access to the console port.



NOTE: In earlier IOS, a type 0 password is one in clear text, which is visible to any user who may access the router in privileged mode. On the other hand, a type 7 password uses a weak, exclusive or type encryption. Because a type 7 password may be retrieved via many of the publicly available password tools, it is not considered secure.

With the Enhanced Password Security feature that comes with later protection. To use this feature, rely on the username secret command to specify a username and its associated MD5-encrypted secret.

Verify network status and router operation using basic utilities (including: ping, traceroute, telnet, SSH, arp, ipconfig), SHOW & DEBUG commands.

For information on these commands please refer to Objective 10 of Chapter 1.

Chapter 5 - Explain and Select the Appropriate Administrative Tasks Required for a WLAN

Describe standards associated with wireless media (including: IEEE WI-FI Alliance, ITU/FCC.)

The Cisco Unified Wireless Network architecture is all about the use of the Catalyst 6500 Series Wireless Services Module (WiSM) to provide centralized management of WLAN and integration of WLAN into the regular Layer 2 and Layer 3 switching/routing platforms. WiSM has to occupy one slot in the Catalyst 6500 series switch. The switch chassis needs a Supervisor 720 module.

IEEE 802.11 defines wireless protocol for Ad-hoc and client/server networks as well as specifications for the physical layer and the Media Access Control layer. In a basic WLAN, an access point (AP) is relied upon to handle traffic from the mobile radio to the wired or wireless backbone of the client/server network. Data is routed between wireless stations or to and from the network server under the AP mechanism.

NOTE: The Institute of Electrical and Electronics Engineers (IEEE) as a non-regulatory body defined the famous 802 standards for networking. On the other hand, the Wireless Ethernet Compatibility Alliance (WECA) is made up of leading wireless equipment and software providers with the goal of guaranteeing interoperability of Wi-Fi products.

LWAPP defines activities related to access point (AP) device discovery, information exchange, and configuration, certification and software control. It also addresses packet encapsulation, fragmentation, and formatting. The communication control and management activities between different APs are also covered. Think of LWAPP as an effort to standardize and centralize WLAN intelligence.

With the Cisco Unified Wireless Network architecture, the Lightweight Access Point Protocol (LWAPP) is used for establishing secure connections between the APs and the various modules across the Layer 3 network.

Know the basics of these standards:

- IEEE 802.11 defines protocol for Ad-hoc and client/server networks as well as specifications for the physical layer and the Media Access Control layer. It does not specify technology or implementation though.
- IEEE 802.11 supports a data rate of Up to 2Mbps in the 2.4GHz band via FHSS or DSSS.
- IEEE 802.11a supports a data rate of up to 54Mbps in the 5GHz band via OFDM.
- IEEE 802.11b supports a data rate of Up to 11Mbps in the 2.4GHz band via DSSS with CCK.
- IEEE 802.11g supports a data rate of Up to 54Mbps in the 2.4GHz band via OFDM (above 20Mbps) or DSSS with CCK (below 20Mbps).
- 802.11b/2.4GHz devices operate in an unlicensed radio band and transmit data on the same frequency as many of the household appliances.

NOTE:	Know that 802.11 will also consist of 802.11, 802.11a, 802.11b, and 802.11g. The most common standard in use today for wireless networks, the 802.11b standard defines DSSS networks that use the 2.4GHz ISM band and communicate at speeds of 1, 2, 5.5 and 11 Mbps. Always remember, the farther away the computer is from an access point directly affects the coverage available, as well as the speed of the connection.

Identify and describe the purpose of the components in a small wireless network. (including: SSID, BSS, ESS.)

IEEE 802.11 is a set of standards developed for wireless local area network (WLAN) computer communication. It was developed by the IEEE LAN/MAN Standards Committee n the 5 GHz and 2.4 GHz spectrum bands. These are considered public spectrum bands. You can configure wireless within these two bands only. Wireless solutions you can choose from include 802.11, 802.11a, 802.11b and 802.11 g.

The basic elements in a WLAN domain are the client, the AP (or Access Point) and the actual coverage area you want to service. The client is considered a WLAN client and/or a station (STA). The client can be a phone, a laptop or any system with a wireless card installed on it. The AP is the centralized concentrator for all wireless communication when not working in Ad Hoc mode. The AP has a specific coverage area which is determined by the size, shape and type of

antennas in use. The coverage area is also known as the Basic Service Set (BSS). An Extended Service Set (ESS) is used to connect multiple Basic Service Sets.

When configuring a WLAN, you should be aware of the basic components that make up a Basic Service Set (BSS). An SSID (Service Set ID) is the name of a wireless local area network (WLAN) in which all hosts will be connected to if they also have the same SSID configured. All wireless devices on a WLAN must use a similar SSID in order to communicate with each other. SSIDs are case sensitive text strings that utilize a sequence of alphanumeric characters (letters or numbers) and can only be a maximum of 32 characters in length.

The IEEE 802.11 standard defines the basic service set (BSS), which is made up of wireless devices communicating with a single Access Point, within a single cell. When no connections back to a wired network exist, this would be called an independent basic service set. When there is a connection to the wired network (via an Access Point), this would be called an infrastructure BSS. When there is no access point in use, it would simply be an ad-hoc network.

Through the use of an extended service set (ESS), your users may move between multiple infrastructure BSSs since the APs may communicate amongst themselves for forwarding traffic from one BSS to another (as well as switching the roaming devices from one to another). The medium involved for carrying out this function used is called the distribution system (DS).

For the CCNA exam you will need to know the differences between an ESS and a BSS. For the exam, you will be expected to know the difference between both and functionality as well as features provided by both. When a wireless communication device uses a single access point (AP) for connectivity to other wired network resources, it is considered a BSS or Basic Service Set. When multiple service sets are joined together via a wired segment, (usually with two or more APs), then you are working within an Extended Service Set or ESS.

When configuring an ESS, you need to make sure that you are not overlapping channels, and if you are, that they are configured in such a way that they do not cause issues with wireless access and use. An ad-hoc network will not suffer from overlap. A service set however (BSS), when overlapped with another service set, could cause duplicate channels to be used. This would cause a network disruption. Some APs can auto-configure their settings to use the least used wireless channels. Overlapping channels in a WLAN can cause connectivity problems because its very similar to ‘overcrowding’ on a wired network. This problem can be resolved by doing a site survey and using non-overlapping channels such as 1, 6, and 11 which do not overlap

Remember the following. Rely on an AP to handle traffic from the mobile radio to the wired or wireless backbone of the client/server network. Data is routed between wireless stations or to and from the network server under the access point mechanism. Generally speaking, WLANs controlled by a central access point can provide higher overall performance.

Infrastructure mode consists of at least one access point that is connected to the wired network infrastructure. A client/server network uses an access point to control the allocation of transmit time for all stations. This architecture allows mobile stations to roam from cell to cell. Note that when one access point is connected to a wired network and a set of wireless stations, it is

referred to as a Basic Service Set (BSS). On the other hand, an Extended Service Set (ESS) refers to a set of two or more BSSs that form a single network segment.

NOTE: With Ad hoc mode (peer-to-peer mode), wireless end stations communicate directly with one another without using access point.

Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point.

Generally speaking an AP can be configured through the GUI, the CLI (through Telnet) or through the console port. Using the GUI is often the preferred option due to ease of use.

To access the AP with the GUI, first assign an IP address to the AP device. This is usually done through DHCP. After address configuration, access the AP through the web browser. The Express Setup window has all the basic parameters that are needed for establishing a wireless connection. The most critical information here includes:

- The AP's host name
- IP address configuration
- Default gateway
- SNMP community string
- SSID

A client needs to know these in order to connect to the correct AP.

Compare and contrast wireless security features and capabilities of WPA security (including: open, WEP, WPA-1/2.)

In WLAN, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server. The server requests that the access point submit proof of identity in order to complete the authentication. The 802.11 WLAN standard makes use of shared-key authentication and static wired equivalent privacy (WEP) keys, which can be easily compromised nowadays.

NOTE: Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks defined in the 802.11b standard. It works at the data link and the physical layers with the aim of providing the same level of security as that of a wired LAN. However, it does not offer end-to-end security, and it is not as secure as once believed. Wired Equivalent Privacy or Wireless Encryption Protocol (WEP) is a scheme to secure IEEE 802.11 wireless networks. It is part of the IEEE 802.11 wireless networking standard. WLANs broadcast

messages using radio frequency (RF) technology. Because of the inherent weaknesses revolving around this technology, wireless can seem more susceptible to eavesdropping than wired networks. Due to this fact, it's imperative that security not be overlooked when deploying a WLAN. The most basic form of security you can use (but not fully recommended) is WEP. WEP, which stands for Wired Equivalent Privacy, is a security encryption method that was intended to secure 802.11 WLANs from attack. Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication. If you use WEP, it should be noted that it is not fully secure. The encryption can be cracked within minutes by freely available tools on the Internet.

An alternative WLAN security approach focuses on providing centralized authentication and dynamic key distribution, which is based on the IEEE 802.11 Task Group "i" end-to-end framework using 802.1X and the Extensible Authentication Protocol (EAP).

NOTE: Extensible Authentication Protocol (EAP) is a general protocol for authentication that supports authentication methods such as token cards, one-time passwords, certificates, smart cards...etc.

The Cisco Wireless Security Suite has the following three security elements:

- Mutual authentication between client and authentication server
- Encryption keys dynamically derived after authentication
- Centralized policy control

EAP-Cisco Wireless (Cisco LEAP) is a widely deployed EAP type for WLANs that supports the security elements previously mentioned.

NOTE: With fast secure roaming, authenticated clients may roam securely at layer 2 from one AP to another, supposedly without any perceptible delay. The feature requires IOS 12.2(11)JA or greater for the Aironet 1200 and the 1100 Series access points. Use it primarily for supporting delay sensitive applications (such as voice applications). Do note that this fast secure roaming feature currently supports up to 30 APs per layer 2 domain only.

Identify common issues with implementing wireless networks.

Radio transmission requires a clear path between antennas. This is known as radio line of sight (LOS), which refers to the direct free-space path that exists between two points. Obstructions that might obscure a visual LOS include mountains and trees, curvature of the Earth, buildings and other man-made objects.

The Fresnel zone is an elliptical area immediately surrounding the visual path. It often varies in thickness depending on the length of the signal path as well as the frequency of the signal.

Keep in mind, WLAN connections may be affected by RF interferences. Sources of RF interference may include microwave ovens, wireless phones, Bluetooth enabled devices and other wireless LANs. In response, analyze the potential for RF interference, prevent the interfering sources from operating, and further provide adequate wireless LAN coverage.

Hidden nodes in a wireless network refer to nodes that are out of range of other nodes. The 802.11 standard relies on RTS/CTS to partly overcome the hidden node problem.

Multipath propagation, on the other hand, is a problem that can occur when an RF signal takes different paths to a destination node due to bouncing in different directions. Under this situation, some (but not all) signal will encounter delay and travel longer paths to the destination node, thus causing the signal to overlap.

NOTE:

<u>Most of these problems can actually be prevented with proper site survey conducted in advance.</u>

Major areas of consideration when designing a WLAN include Range and Coverage, Data Rate and Capacity, Interference Immunity, and Connectivity and Power Requirements. The goal of a RF site survey is to acquire sufficient information to determine the number and placement of access points that provides adequate coverage throughout the facility. The need and complexity of the survey does vary, largely depending on the facility being investigated.

Typical steps for RF survey include:

1. Obtaining a facility diagram
2. Visually inspecting the facility
3. Identifying user areas
4. Determining preliminary access point locations
5. Verifying access point locations
6. Documenting findings

Chapter 6 - Identify Security Threats to a Network and Describe General Methods to Mitigate Those Threats

Explain today's increasing network security threats and the need to implement a comprehensive security policy to mitigate the threats.

Information security is not a one-off initiative, but an ongoing process that needs to be continuously managed. Effective information security management is a business requirement. By aligning security objectives with business objectives one can enable senior management to understand and support IS initiatives.

Information security protects valuable information assets against loss, operational discontinuity, misuse, unauthorized disclosure, inaccessibility, or damage. In order to protect the interests of those relying on information, the key concerns of availability, confidentiality, integrity, authenticity and non-repudiation must be addressed. The relative priority and significance of these concerns may vary according to the data within the information system and the corresponding business context.

Internet poses significant security problems for organizations when protecting their information assets. The areas of control against internet threats are policies and procedures, firewall, intrusion detection systems, and other security controls. We will deal with these topics in the coming sections

NOTE: A security policy is relied upon to specify the type of communications allowed, and how connections will be authenticated and protected. Such a policy is needed in a campus network. Technical solutions should follow this policy to the fullest extent.

User awareness is the key to successful security implementation. A security policy will work only if the users understand what they should do and that they are willing to cooperate.

Do keep in mind, whenever dealing with network security the Cisco way, know the SAFE blueprint as well as the new Self Defending architecture. SAFE is a security blueprint for making networks more secure. A design should follow SAFE as closely as possible. It provides a set of objectives to guide in the decision making process during network design. These objectives emphasize security and attack mitigation based on policy, among other principles. On the other hand, the Self Defending Network architecture can be thought of as the successor to SAFE. It emphasizes integration of security throughout the entire network with collaborative processes taking place between various network elements. Such an architecture should be able to adapt to new threats. It works by ensuring resiliency across everything on a network.

NOTE:

SAFE objectives emphasize security and attack mitigation based on policy; security implementation throughout the infrastructure; secure management and reporting; authentication and authorization of devices, users, and administrators to critical network resources; intrusion detection and prevention for critical resources and subnets; and support for emerging networked applications.

The Self Defending Network architecture has 3 phases, which are Integrated Security, Collaborative Security, and Adaptive Threat Defense. There is a heavy emphasis on the network admission control architecture to defend against malware intrusions. There is also a focus on the integration of and collaboration between the intrusion prevention system (IPS), the Security Agent, the CS-MARS (Security Mitigation Analysis and Response System), the CSM (Security Manager) and the SSL based VPN technologies.

Explain general methods to mitigate common security threats to network devices, hosts, and applications.

From a threat perspective, there are internal threats (internal users who need access out) and external threats (external users who need access in). Several common threats are good enough to render an initial compromise that an attacker needs to penetrate the network with secondary exploits.

Therefore, a comprehensive security policy is necessary to serve as the foundation of the security efforts. To be sufficiently comprehensive, the policy must address both the physical and logical sides of the story. Physical security is often part of a critical part of security policy. Related access control includes practices such as restricting entrance to authorized personnel only. One may implement physical access control through a human guard or a mechanical lock or any other fancy ways. On the other hand, the logical side of the story usually addresses different AAA elements across different layers, with layer 2 and layer 3 being the most critical layers to protect.

NOTE: A practical security policy should include (and not limited to) the following elements: the security objectives for an organization, the resources needing protection, the network infrastructure with current maps and inventories, and the critical resources that need extra protection.

Security policy and baselines have to be developed and implemented on the basis of identified and prioritized information resources that need protection. It is impossible to protect everything. Protection has to be done selectively due to resource constraints.

Generally speaking, a switch has no knowledge on and does not care about layer 3 addressing information such as IP addresses, so it is kind of "isolated" from those outside hackers on the internet. HOWEVER, the belief that a layer 2 device is more secure than a layer 3 device is being described by Cisco as a myth. In fact, as suggested in various Cisco tech support documents, the primary threats to the devices at layer 2 are access network are denial-of-service (DoS) attack and spoofing attack.

Spoofing could be an issue both at layer 2 and layer 3. At layer 2 the MAC addresses can be spoofed. At layer 3 the IP addresses can be spoofed too. Because there are activities that map layer 3 addresses to the layer 2 addresses and vice versa, spoofing can in fact be a cross layers issue (a big one indeed).

NOTE: Spoofing could be an issue both at layer 2 and layer 3. At layer 2 the MAC addresses can be spoofed and at layer 3 the IP addresses can also be spoofed. A spoofing attack is an attack in which an attacker (hacker) successfully masquerades as another (person, IP address, MAC address, etc) to gain entry, or to perform other malicious activity.

Different from a switched network, a routed network can associate a logical addressing structure to a physical infrastructure. Therefore, traffic flow on routed networks is inherently different from traffic flow on switched networks. Routed networks have more flexible traffic flow due to the use of the hierarchy to determine optimal paths depending on dynamic factors such as network congestion.

Within any networked host there is a routing table with information stored for determining which physical interface address to use for outgoing IP datagrams. If a host receives an IP datagram on any of its interfaces, there are two possibilities:

- If the datagram is intended for that host, it will be passed to the relevant application on the host.
- If the datagram is addressed to some other hosts, it will be re-transmitted on one or other of the available interfaces.

Just like any networked host, a router has its own routing table too. The routing table entries can be corrupted with spoofed IP addresses. Traffic flows can also be corrupted with spoofed source IP addresses.

With content-addressable memory (CAM) overflow attack, the switch's CAM table is sent a frame with an unknown destination, causing the switch to broadcast frames to everywhere within its Layer 2 domain. If too many frames are like this, the CAM table limit can be exceeded, thus leading to strange behaviors on the switch.

To work against the CAM table overflow attack, it is necessary to configure port security. The drawback of specifying MAC addresses is that it would be way too difficult to manage. It is an option, however, to choose to limit the number of max possible MAC addresses on the switch port. This can be done via the set port security command on the switch.

NOTE:	With a content-addressable memory (CAM) overflow attack, the switch's CAM table is sent a frame with an unknown destination, causing the switch to broadcast frames to everywhere within its Layer 2 domain. If too many frames are sent in this format, the CAM table limit can be exceeded. If the CAM table limit is exceeded, problematic behavior may result.

With DoS attacks against the Spanning Tree Protocol (STP), the stability of the entire spanning tree topology can be compromised when one host in the topology impersonates a bridge and sends BPDUs to the network. The attacks lead to unnecessary spanning tree calculation on a port, which can take up to 30 seconds to complete before operation can turn back to normal.

NOTE:	By default, Spanning Tree Protocol (STP) does not provide mechanisms for security so enhancements have been made. To mitigate STP manipulation, do the best in enforcing the placement of the root bridge and the domain borders. This can be done via the root guard/BPDU guard enhancement commands. The administrator can set the root bridge priority to 0 in an effort to secure the root bridge position. But there is no guarantee that if a bridge with a priority of 0 and a lower MAC address is added that the current root bridge won't be disrupted. By implementing the root guard feature, you can securely enforce your root bridge placement in the network. The root guard ensures that the port on which root guard is enabled

is the designated port. BPDU guard is similar in nature. By implementing BPDU guard, a port can be disabled once a BPDU is received. The Portfast feature must also be enabled for BPDU guard to function.

To work against Spanning Tree Protocol manipulation, do the best in enforcing i, placement of the root bridge and ii, the domain borders. This can be done via the root guard/BPDU guard enhancement commands.

NOTE: Port security could be the best tool against spoofing attacks.

There are other attacks (layer 2 attacks, layer 3 attacks or a mixture of both) that may require more sophisticated monitoring and detection solutions to defend against. Netflow is one possible option.

A network flow refers to an unidirectional sequence of packets between a given source and destination endpoints. Network flows are usually highly granular, with flow endpoints identified both by an IP address and the transport layer application port numbers. In addition, NetFlow also uses the IP type and the input interface identifier to uniquely identify flows.

NetFlow statistics is a global traffic monitoring feature that allows monitoring of all IPv4-routed traffic at the flow-level. Collected statistics can be exported to an external device for further analysis. In combination with the appropriate Catalyst switch Supervisor Engine, NetFlow can even report VLAN statistics for routed traffic in and out of a VLAN as well as other Layer 2 output VLAN statistics. Excessive flooding of frames in the VLANs, for example, could well indicate attack-in-progress.

NOTE: Another major source of threat come from worm, virus and Trojan horse:

- Non-capable of self-replication, a Trojan horse is a destructive program that masquerades as a benign application.
- A computer virus is a program that attaches itself to another program or file so that it can spread from one computer to another. In other words, it does not spread by itself but through the help of the others.

- A worm is similar to a virus because it can spread from computer to computer. However, it can spread out without any help from any third party program or file.

These attack methods often spread through email attachments and file exchanges (such as FTP). In fact FTP is often the target of hacking attempts. Isolate the public FTP servers from the internal network by having them placed in a perimeter network. Also closely monitor the activities over TCP ports 21 and 20.

Describe the functions of common security appliances and applications.

Packet Filtering

A Cisco router may serve as a basic packet filter through its basic traffic filtering capabilities with access control lists (ACLs). ACLs work by controlling whether routed packets are forwarded or blocked at the router's interfaces. Direct the router to examine each packet to determine whether to forward or drop the packet, on the basis of the criteria specified within the ACLs. Valid criteria may include the source address of the traffic, the destination address of the traffic, the upper-layer protocol, and other information. ACLS can be configured for all routed network protocols to filter the packets of those protocols as the packets pass through a router.

From a practical standpoint, use ACLs to provide a basic level of security for accessing the network. Without proper ACLs configured, all packets passing through the router could be allowed onto all parts of the network. At the minimum, configure ACLs on the border routers to provide a basic buffer from the outside network or from a less controlled area of the private network into a more sensitive area of the private network. On these routers, configure ACLs for each network protocol configured on the router interfaces. Ideally, both the inbound traffic and the outbound traffic should be filtered on an interface if the performance tradeoff is justified.

Do keep in mind that router ACLs are never sophisticate enough for protecting the network against intentional hacking attacks. If the network is a popular attack target, consider to install a full blown firewall or deploy the advanced IOS firewall features instead.

NOTE:

To create a very basic access list, the following elements need to be specified:

- The protocol to filter
- A unique name or number of the access list
- Packet filtering criteria

Do keep in mind that access lists of some protocols must be identified by a name, and access lists of other protocols must be identified by a number. Some protocols can be identified by either a name or a number. As said before, however, only numbers are required for the purpose of this exam.

Also note that even though most of the time the packet source addresses, packet destination addresses, and upper-layer protocol as the filtering criteria will be used, each protocol does have its own specific set of criteria that best fits certain purposes. For the purpose of this exam, however, the primary focus should be on the IP access list.

There can be up to 99 Standard IP access lists ranging in number from 1 to 99. It is also possible to have up to 100 Extended IP access lists ranging in number from 100 to 199. A Standard access list only permits or denies traffic from specific IP addresses, regardless of the destination of the packet and the ports involved. Extended access lists, on the other hand, allow for the permitting or denying of traffic from specific IP addresses to a specific destination IP address and port. It is also possible to specify different types of protocols for more granular control of traffic flows.

Proxying

A proxy server intercepts all messages entering and leaving the network. It is more like a middle man – it makes outgoing requests on behalf of the insiders so the insiders are never exposed to the outside risks directly. Most proxy servers are software based. They usually provide caching facilities to speed up internet access in the case of network congestion.

Firewalling

A firewall prevents unauthorized access to or from a private network by examining each message that passes through it and blocks those that do not meet the specified security criteria. It may be implemented in hardware or software, or a combination of both. If using Cisco only solutions, it is possible to either use the PIX firewall products or the IOS Firewall Feature set, which works not only on routers but also on certain Catalyst switches that are equipped with the firewall

feature set images. Supported features may include Context-Based Access Control (CBAC), Authentication Proxy and Port-to-Application Mapping (PAM).

NOTE: When going through the secure network lifecycle phases it is possible to come across the need for dealing with the issue of firewall deployment. The evaluation of network infrastructure security often involves the protection of network-accessible resources from unauthorized use. Start by authenticating the user. Once authenticated, use firewall to enforce access policies. Do note that defending against unauthorized access through firewall alone could not stop potentially harmful contents from being transmitted, unless deploying specific technology to prevent this.

Stateful Inspection of ICMP traffic is supported in the Cisco IOS firewall (first introduced in 12.2(11)YU). With stateful inspection, the firewall can track the state of network transactions and then act accordingly. Do note that stateful inspection of ICMP packets is restricted to those most commonly used types of ICMP messages only.

NOTE: The inspect command can be used with a policy map to enable IOS stateful packet inspection.

Stateful inspection is particularly useful for defending against SYN attack, which occurs when a network is weighed down with packets initiating incomplete connection requests that, it can no longer process genuine connection requests. The host's memory buffer is eventually filled up, and network service becomes totally interrupted.

Cisco IOS Firewall maintains a so-called session state table for controlling the security of inspected connections. There is also a term known as Adaptive Security algorithm, which is a stateful approach to security. Based on this algorithm, no packets would be allowed to traverse the Firewall without a valid connection and state (i.e. application-layer protocol session information).

NOTE: With the Adaptive Security Algorithm (ASA), ICMP packets are almost always denied unless specifically permitted.

The CBAC (Context Based Access Control) functionality makes use of session state information to intelligently filter TCP and UDP packets. TCP and UDP traffic would be allowed through the firewall only when the connection is initiated from a private network (meaning the return traffic is likely legitimate). Without this feature, filtering would have to be limited to ACLs that examine packets at the network or transport layer.

NOTE: The CBAC feature inspects packet sequence numbers in the active TCP connections to determine if they are within or out of the expected ranges. Suspicious packets and half-open connections may be dropped based on the specification.

There is also a feature known as Stateful Failover, which supports active or standby failover for most types of TCP traffic. This feature is formally supported on 3700, 3800, and 7200.

Intrusion Detection and Prevention

Intrusion detection system (IDS) / Intrusion Prevention System (IPS) can be broadly classified into the following:

- In a network-based IDS system, individual packets that flow through a network are analyzed.
- In a host-based IDS system, activities on each individual computer are individually inspected.
- In a passive IDS system, the IDS detects potential security breaches and raise alerts proactively.
- In a reactive IDS system, the IDS reactively responds to any suspicious activity through logging off the involved user and blocking network traffic from the suspected source.

A complete network sensing solution the Cisco way is network based and can be configured to act “passively” and/or “reactively”. The solution involves at least a sensor, the detection module itself, and possibly a router running the IOS IPS as well as some line-card modules. Sensing platforms are the key components of the IPS and are typically managed via the IPS MC. Note that sensors up to versions 4.x are called IDS sensors, while later sensors are called IPS sensors.

The IOS IPS feature closely monitors packets and sessions that pass by the router. It is recommended to have it running at the network edge to prevent malicious traffic from passing the network border.

When suspicious activity is detected, IPS stops it prior to the occurrence of any damage. Logging of such event may be conducted via IOS syslog messages or through the Security Device Event Exchange (SDEE), which refers to the application-level protocol that exchange IPS messages between the IPS clients and the IPS servers. It is a protocol that is always running, even though it will not process events from an IPS unless SDEE notification has been explicitly been turned on.

NOTE: You can use Intrusion Detection to mitigate attacks. An IDS unit (which stands for Intrusion Detection System) is used to detect malicious attempts at protected computer systems. It's a form of scanner that will look for anomalies in your systems, data traffic and so on, in an attempt to flag these anomalies in order to warn you of attack. Some units can even take action such as sending alerts. An IPS unit (which stands for Intrusion Prevention System), will monitor the systems or network in order to catch malicious attempts in real time so that the issue can be not only flagged, but action is taken immediately to prevent an attack -not just warn of it.

Virtual Private Networking

VPN is a private network that uses the Internet to connect remote sites or users together in a highly secure manner (through encryption of traffic in-transit). The two common types of VPNs are:

- Remote-Access - a Virtual Private Dial-up Network (VPDN) for user-to-LAN connection

- Site-to-Site - for connecting multiple fixed sites through the use of dedicated equipment and large-scale encryption

IP Security (IPSec) is a framework of open standards for data confidentiality, data integrity, and data authentication between the participating peers through secure tunnels. It is required to have it implemented if inter-campus communications are to be supported (in the form of site to site VPNs).

The IOS implementation of IPSec supports AH and ESP. Do note that IPSec can be applied only towards unicast IP datagrams. If NAT is currently in place, static NAT translations must be configured for IPSec to work properly.

Describe security recommended practices including initial steps to secure network devices.

The evaluation of network infrastructure security often involves the protection of network-accessible resources from unauthorized use.

- Start by authenticating the user. Once authenticated, use firewall to enforce access policies. Do note that defending against unauthorized access could not stop

potentially harmful contents from being transmitted, unless deploying specific technology to prevent this.

- Following authentication, control access carefully. Logical access control refers to the policies and procedures together with the underlying organizational structure and electronic access controls that are put together for restricting malicious or disallowed access to computer resource. An effective security control system should ensure that the objectives of operation effectiveness, reliability and efficiency can be fully achieved through measures that take care of issues such as authentication, authorization and audit.

NOTE:	Identity-Based Networking Services, or IBNS, integrates authentication, access control, and user policies for securing network connectivity and resources. It has policies associated with users instead of physical ports so users may enjoy more mobility. In terms of administration, it emphasizes the use of centralized policy based administration rather than local decentralized management. At present IBNS together with 802.1x are supported on certain Catalyst switches (6500, 4500, 3550, and 2950 switches) and on the Cisco ACS (Access Control Server) Server/Aironet Access Points.

As an architectural framework for configuring security functions in a consistent manner, AAA provides guidance through which access control is set up on the router. With AAA, the type of authentication and authorization desired on a per-line, per-user or per-service basis can be dynamically configured. It allows one to define authentication and authorization through method lists, then applying those method lists to the specific services or interfaces.

Authentication refers to the process of validating the claimed identity of an end user or a device – it authenticates not only human users, but also devices. Authorization refers to the act of granting access rights. It provides the ability to limit network services to different users via dynamically applied access list. Accounting refers to the methods to establish who (or what) performed a certain action. In fact, the accounting function may be used for connection time billing. It may also be used to track suspicious connection attempts into the network.

Chapter 7 - Implement and Verify WAN Links

Describe different methods for connecting to a WAN.

WAN protocols supported by most Cisco gears include Asynchronous Transfer Mode (ATM), Frame Relay, High-Level Data Link Control (HDLC), Integrated Services Digital Networks (ISDN), Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Switched Multimegabit Data Service (SMDS), X.25 and its derivatives.

Practically speaking, WAN services are typically provided through several primary switching technologies, which are Circuit switching, Packet switching and Cell switching. Each of these switching techniques has advantages as well as disadvantages.

Branch Office WAN Solutions

Use slow modem dial up access for small remote offices with very few users. The idea is to pay only for actual use, although modem connection tends to be buggy. ISDN should be considered if something better is desired.

NOTE: Basic Rate Interface (BRI) ISDN consists of two 64-Kbps B-channels plus one D-channel for transmitting control information. The Cisco 800 series routers provide secure ISDN access to the Internet and the corporate LAN.

Dialer profiles allow logical and physical configurations to be bound together on a dynamic and per call basis, thus allowing physical interfaces to take on different characteristics based on incoming/ outgoing call requirements.

Access Network Solutions for a Teleworker

Cable modems are designed to operate over cable TV lines. By leveraging the cable TV infrastructure more remote users can have access to the internet. Hybrid Fiber-Coaxial (HFC) was in use by cable TVs for two-way access using fiber optics together with coaxial cable. The network extends from a central location to each headend and then to a hubsite. The fiber optic node down the link provides services to max 2000 nodes.

Digital subscriber lines (DSL) are last-mile technologies that use special modulation schemes to pack data onto copper wires of the PSTN network. They can offer speeds as high as 32 Mbps for upstream traffic and from 32 Kbps to over 1 Mbps for downstream traffic.

ADSL uses an upstream band (from 25.875 kHz to 138 kHz) and a separate downstream (from 138 kHz to 1104 kHz) band. ADSL2 is capable of providing a higher downstream rate. In addition to ADSL, there are other DSL implementations, including:

- HDSL can deliver 1.544 Mbps of bandwidth each way over two copper twisted pairs with a max operating range of 12,000 feet.
- IDSL transmits data digitally across existing ISDN lines at a rate of 128 Kbps.
- SDSL delivers 1.544 Mbps both downstream and upstream over a single copper twisted pair with a max operating range of 10,000 feet.
- Cisco Long Range Ethernet (LRE) uses Very High Data Rate Digital Subscriber Line (VDSL) technology to extend Ethernet services over existing twisted pair wiring at speeds from 5 to 15 Mbps and distances up to 5,000 feet.
- To allow users to connect to the network via DSL, configure and activate PPPoE.

Remote Data Center WAN solutions

A typical enterprise data center has a network with a three-tier design: an Ethernet access layer, an aggregation layer and the campus core layer. For a remote data center to function as expected, the WAN connection between it and the user end must be stable, fast and secure.

Different types of WAN links deploy different control methods. WAN load balancing and other traffic queuing mechanisms can be used to manage traffic for better bandwidth utilization. To maintain a remote data center, stable, consistent and reasonably fast connections are required. Use cable modems, DSL, etc… for this purpose. Frame Relay may be a relatively better choice if stability and consistency are preferred.

Frame relay switches multiplex data on shared lines asynchronously as quick as they can without correcting any corrupted data or waiting for any acknowledgment. Frame relay connects over Permanent Virtual Circuits (PVCs) rather than physical circuits. Each PVC has a burst rate and a Committed Information Rate (CIR), which represents a service provider commitment on available bandwidth. Since frame relay shares infrastructure among multiple users, it is a cost-effective approach for connecting remote LANs to the backbone.

Configure and verify a basic WAN serial connection.

On the 2500 you may setup serial WAN connection using the serial ports at the back.

Point-to-Point Protocol (PPP) is one method of connecting a computer to a remote network. It works at the data link layer, is more stable than SLIP and has error-checking features included. Do note that both SLIP and PPP encapsulate datagrams and other network-layer protocol information over point-to-point links, and that PPP negotiation consists of three phases, which are Link Control Protocol (LCP), Authentication, and Network Control Protocol (NCP).

Asynchronous interfaces correspond to physical terminal (TTY) lines. Commands can be entered in asynchronous interface mode to configure protocol-specific parameters for asynchronous interfaces. Commands can also be entered in line configuration mode to configure the physical aspects of the same port. Note that the type of modem attached to the router can be discovered with the modem autoconfigure discovery line configuration command. Another option is configuring the modem automatically with the modem autoconfigure type modem-name line configuration command.

NOTE: WAN Manager is a UI for managing WAN links. It can be used if dealing with the configuration of more complicated WAN links.