STUDY GUIDE

Cisco

640-816

CCNA ICND (Part II)

ExamForce

About the Exam

There are five major topic areas or domains that make up this exam:

- Configure, verify and troubleshoot a switch with VLANs and interswitch communications.
- Implement an IP addressing scheme and IP Services to meet network requirements in a medium-size Enterprise branch office network.
- Configure and troubleshoot basic operation and routing on Cisco devices.
- Implement, verify, and troubleshoot NAT and ACLs in a medium-size Enterprise branch office network.
- Implement and verify WAN links.

This guide will walk you through all of the technologies in the objectives and sub-objectives.

Objectives

Chapter 1: Configure, verify, and troubleshoot a switch with VLANs and interswitch communications

Describe enhanced switching technologies (including: VTP, RSTP, VLAN, PVSTP, 802.1q).

Describe how VLANs create logically separate networks and the need for routing between them.

Configure, verify, and troubleshoot VLANs.

Configure, verify, and troubleshoot trunking on Cisco switches.

Configure, verify, and troubleshoot interVLAN routing.

Configure, verify, and troubleshoot VTP.

Configure, verify, and troubleshoot RSTP operation.

Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network.

Implement basic switch security (including: port security, unassigned ports, trunk access, etc.)

Chapter 2: Implement an IP addressing scheme and IP Services to meet network requirements in a medium-size Enterprise branch office network

Calculate and apply a VLSM IP addressing design to a network.

Determine the appropriate classless addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment.

Describe the technological requirements for running IPv6 (including: protocols, dual stack, tunneling, etc)

Describe IPv6 addresses.

Identify and correct common problems associated with IP addressing and host configurations.

Chapter 3: Configure and troubleshoot basic operation and routing on Cisco devices

Compare and contrast methods of routing and routing protocols.

Configure, verify, and troubleshoot OSPF.

Configure, verify, and troubleshoot EIGRP.

Verify configuration and connectivity using ping, traceroute, and telnet or SSH.

Troubleshoot routing implementation issues.

Verify router hardware and software operation using SHOW & DEBUG commands.

Implement basic router security

Chapter 4: Implement, verify, and troubleshoot NAT and ACLs in a medium-size Enterprise branch office network

Describe the purpose and types of access control lists.

Configure and apply access control lists based on network filtering requirements.

Configure and apply an access control list to limit telnet and SSH access to the router.

Verify and monitor ACLs in a network environment.

Troubleshoot ACL implementation issues.

Explain the basic operation of NAT.

Configure Network Address Translation for given network requirements using CLI

Troubleshoot NAT implementation issues

Chapter 5: Implement and verify WAN links

Configure and verify Frame Relay on Cisco routers

Troubleshoot WAN implementation issues

Describe VPN technology (including: importance, benefits, role, impact, components)

Configure and very PPP connection between Cisco routers

Chapter 1 - Configure, Verify, and Troubleshoot a Switch with VLANs and Interswitch Communications

Describe enhanced switching technologies (including: VTP, RSTP, VLAN, PVSTP, 802.1q).

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. Therefore reducing the need to configure the same VLAN everywhere. VTP is Cisco-proprietary and is available on most of the Cisco Catalyst Family products.

The Inter-Switch Link (ISL) protocol is used to interconnect two VLAN-capable switches (and routers). As a packet-tagging protocol, ISL contains a standard Ethernet frame and the VLAN information associated with that frame. The packets on the ISL link contain a standard Ethernet, FDDI, or Token Ring frame and the VLAN information associated with that frame. At present, ISL is supported only over Fast Ethernet links, but a single ISL link can still carry different protocols from multiple VLANs.

NOTE: For the exam, you will be tested on your ability to understand the finer details of VLANs, VTP, trunking and Spanning Tree Protocol (STP). You will need to know how to solve problems within scenarios using any number of multiple technologies all at once. That being said, it's imperative that you understand how all of the switching technologies interoperate. For example, understanding how a VLAN operates at Layer 2 of

the OSI model and how a Layer 3 interface (and IP address) allow intra-subnet routing. Understanding how mis-configuring your VTP parameters can propagate false VLAN information throughout your network is also important. For the exam you will need to understand how Spanning Tree Protocol (STP) works to keep your switched environment stable when you have redundant links. All of this and more will be tested on the exam, make sure you visit Cisco's main website and their documentation and review all of the basic of switching before taking the exam.

As part of the IEEE 802.1 standard for media access control bridges, the Spanning Tree Protocol (STP) is a link management protocol that implements the spanning tree algorithm for providing path redundancy while preventing undesirable loops in a network that are created by multiple active paths between hosts. Rapid Spanning Tree Protocol (RSTP) can be thought of as an enhanced STP, which gives faster convergence after a topology change. Per-VLAN Spanning Tree (PVST), on the other hand, allows for the maintaining of a spanning tree instance for every individual VLAN configured on the network.

When working with STP (802.1d), you need to know how the Root and Designated ports are selected per segment. For each link between switches (if redundant or not), you need to figure out which end of the switched link will be the Designated port. The Designated port is the one with the lowest Root Path Cost configured. When deploying STP, the first action that will take place will be the 'selection' of the root bridge and this is selected by finding the switch on your network with the lowest-value bridge identifier. This can also be configured statically. This should be a switching device in the center/core of your infrastructure. Once the Root Bridge is selected, the root port on all other bridges is determined. A bridge's root port is the port through which the root bridge can be reached with the shortest root path (least aggregate) cost. Once this is determined, then the Designated bridges/switches and their designated ports are determined. The Designated Bridge is the switch on each network segment that provides the minimum root path cost. A networks designated bridge/switch is the only switch on that segment that will forward frames. The networks designated port is the port that will connect directly to the Designated Bridge.

Describe how VLANs create logically separate networks and the need for routing between them.

Network segmentation

One way to enhance the efficient of a network is to have it properly segmented. There are two benefits in restricting broadcast traffic to a small local segment. First, it becomes possible to avoid wasting bandwidth. Second, 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 has been reached, routers can be added to it in order to create new segments and allow additional hosts to join in.
2. Segmenting the network reduces the number of hosts per network and therefore reduces the frequency of collision.
3. Dividing a big network into multiple smaller segments reduces the overflow of problems from one segment to the next.
4. Utilizing segments ensures 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

It is possible to have segments interconnected by routers to enable communication between LANs while blocking other types of traffic. Routers can 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 and VLANs

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 can 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. And since that communication between VLANs is mostly accomplished through routing, most traditional security and filtering functions of the Cisco routers can be deployed.

Configure, verify, and troubleshoot VLANs.

Inter-Switch Link Protocol

Under ISL, an Ethernet frame is encapsulated with a header that transports VLAN IDs between switches and routers. A 26-byte header (which includes a 10-bit VLAN ID) is pre-pended to this Ethernet frame. Note that the VLAN ID is added to the frame only when the frame is destined for a non-local foreign network.

Do note that ISL support is hardware-dependent for the Catalyst switches. Therefore, when connecting an external router to a Catalyst switch, first use one of the following commands to determine the encapsulation support per module:

- In CatOS, use **show port capabilities**
- In IOS, use **show interfaces capabilities**

VLAN troubleshooting

A VLAN consists of several end systems, all of which are members of a single logical broadcast domain. It is supported on various pieces of network equipment that support VLAN trunking protocols (VTP) between them. Therefore, problematic VTP configuration can lead to problems in the VLAN.

Before a port has 802.1q trunking turned on, it belongs to a single VLAN. When trunking is on, the port can carry traffic for many VLANs, even though it will still remember the VLAN it was in before trunking was turned on (i.e. the native VLAN). If the native VLAN on each end of the link does not match, a port will go into a Disable state due to a mismatch error (certain Catalyst switches may shut down the port if software processes inside the switch detect an error).

Another possible cause of inactive ports is when the VLAN these ports belong to have disappeared. Each port in a switch belongs to a VLAN. If that VLAN is accidentally deleted, then the port will become inactive. Some switches show a steady orange light on each inactive port. To fix the problem, simply add the VLAN back into the VLAN table.

To configure a specific VLAN, use the **vlan** command in VLAN configuration mode. To delete a VLAN, use the no form of the same command. To enter VLAN configuration mode, use the **vlan database** command under privileged EXEC mode. The **show vlan** command can be used to tell what information has been configured for the VLAN.

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.

NOTE: For the CCNA exam you will need to know the fundamentals of network switching at Layer 2 of the OSI Model as well as the functional aspects of the trunking of switch links. When working with trunking, you can use ISL or 802.1Q. When working with 802.1Q, all VLAN packets sent are tagged from the trunk port – all except the native VLAN. Native VLAN packets are sent untagged on the trunk link. By default, VLAN 1 is the native VLAN on all switches. When designing your switched network, it is important to properly plan for the native VLAN, especially if you are relying on the tagged aspects of each frame sent through the trunk. When configuring both switches, make sure that the native VLAN is the same for trunking and tagging purposes. If you configure this properly, you will be able to monitor your network and figure out from which VLAN a frame belongs when you receive a frame with no tag.

VLAN Frame Tagging

VLAN switching relies primarily on frame tagging, which is a mechanism that requires traffic originating and contained within a particular virtual topology carries a unique VLAN ID as it traverses a common backbone or trunk link. The VLAN ID enables VLAN switching devices to make intelligent forwarding decisions.
Each VLAN on a network is differentiated by a "color", which is actually a VLAN identifier. The "frame coloring" of a VLAN is determined by the VLAN ID. Packets originating and contained within a particular VLAN carry the identifier that uniquely defines that VLAN.

The VLAN ID allows the VLAN switches (and routers) to selectively forward packets to ports with the same VLAN ID. The switch that receives the frame inserts the VLAN ID and the packet is switched onto the shared backbone network. When the frame exits the switched LAN, a switch strips the header and forwards the frame to the matching interfaces based on the VLAN color.

Inter-Switch Link Protocol

Under ISL, an Ethernet frame is encapsulated with a header that transports VLAN IDs between switches and routers. A 26-byte header (which includes a 10-bit VLAN ID) is pre-pended to this Ethernet frame. Note that the VLAN ID is added to the frame only when the frame is destined for a non-local foreign network.

Do note that ISL support is hardware-dependent for the Catalyst switches. Therefore, when connecting an external router to a Catalyst switch, first use one of the following commands to determine the encapsulation support per module:

- In CatOS, use **show port capabilities**
- In IOS, use **show interfaces capabilities**

VLAN troubleshooting

A VLAN consists of several end systems, all of which are members of a single logical broadcast domain. It is supported on various pieces of network equipment that support VLAN trunking

protocols (VTP) between them. Therefore, problematic VTP configuration can lead to problems in the VLAN.

Before a port has 802.1q trunking turned on, it belongs to a single VLAN. When trunking is on, the port can carry traffic for many VLANs, even though it will still remember the VLAN it was in before trunking was turned on (i.e. the native VLAN). If the native VLAN on each end of the link does not match, a port will go into a Disable state due to a mismatch error (certain Catalyst switches may shut down the port if software processes inside the switch detect an error).

Another possible cause of inactive ports is when the VLAN these ports belong to have disappeared. Each port in a switch belongs to a VLAN. If that VLAN is accidentally deleted, then the port will become inactive. Some switches show a steady orange light on each inactive port. To fix the problem, add the VLAN back into the VLAN table.

Redundant topology eliminates single points of failure obviously, but caveats do exist. Redundant topology causes broadcast storms, multiple frame copies, and MAC address table instability problems as examples of what could happen if not configured correctly, or managed properly. In a redundant topology, multiple copies of the same frame can arrive at the intended host, potentially causing problems with the receiving protocol. Common issues resulting from a redundant topology are broadcast storms and instability in the switching tables/databases. A broadcast storm is when each switch on a redundant network floods broadcast frames with no end to the loop and an unending TTL. When you receive multiple copies of a frame arriving on different ports of a switch, you are experiencing a problem known as MAC table or MAC database instability.

Configure, verify, and troubleshoot trunking on Cisco switches.

With VLAN trunking, one single network adapter may behave as a number of virtual adapters (the theoretical limit is 4,096 but a limit of 1,000 is advised for practicality purposes).

NOTE:	For VLAN Trunking to work the network switch, network adapter, and OS, drivers must support VLAN tagging.

IOS based Cisco gear that support trunking include:

- The 2900 Series
- The 2948 (Non L3)
- The 2950 Series
- The 3548
- The 3550 Series
- The 6500

Don’t worry about the CatOS counterparts. The exam does not really care too much about the CatOS based gears.

The two most important commands for setting trunking on IOS based switches are:

- **Switchport mode trunk** allows for the setting of the port to trunking mode.
- **Switchport trunk encapsulation dot1q** allows for the setting of the trunk type to 802.1q (if having to choose between ISL or 802.1q).

Configure, verify, and troubleshoot interVLAN routing.

When a host in one VLAN has to communicate with a host in another VLAN, the traffic needs to be routed. If routing it through the Catalyst switches, create Layer 3 interfaces (known as Switch virtual interfaces SVI) on them. On these switches the VLAN interfaces must be configured with valid IP address. When one switch receives a packet heading for another VLAN, this switch will look into the routing table to determine how to proceed with forwarding the packet. The packet is then passed accordingly.

To troubleshoot, first verify that there is Layer 2 connectivity. Initiate a ping from a host to the switch's corresponding VLAN interface. Next, initiate a ping to the VLAN interface on another VLAN. This is to verify that the switch does properly route between VLANs. Then, initiate a ping from one VLAN to the destination in another VLAN.

If connectivity problem arises, verify that the default route on the switch does point to the correct "default gateway". Also remember to verify that the corresponding IP address and subnet mask on the switch have been correctly configured

Configure, verify, and troubleshoot VTP.

A VTP domain is made up of one or more interconnected switches that share the same VTP domain name. Possible VTP modes include Server, Client, and Transparent.

A switch in the VTP domain sends periodic advertisements out each trunk port. These advertisements are received by neighboring switches for updating the VTP and VLAN configurations. VTP pruning may reduce network bandwidth use by cutting down unnecessary flooded traffic, including broadcast, multicast, unknown, and flooded unicast packets.

There are 2 possible methods that can be used to configure VTP. Configuration through the global configuration mode method is not available in earlier Catalyst switches running IOS, so a better option may be to do it through the database mode. First, enter VLAN configuration mode via the command **vlan database**. Then, set the VTP domain name **via vtp mode {client | server | transparent}.**

Note that all switches involved should have the same the VTP domain name, and that all switches in the concerned VTP domain must run the same VTP version, via matching VTP password. Also note that VTP version 2 is disabled by default on version 2-capable switches.

NOTE: You should always take certain precautions when working on a production network. Any changes you make could impact the current network and halt production. When redeploying an older switch to a new VTP domain in your network you should always take steps to verify that the VTP revision number is lower than the existing domain otherwise the current VTP domain information may be overwritten with that of the older switch. If they do not match, then you will impact the VTP service on the current switched infrastructure.

In order to display the relevant VLAN configuration information such as VLAN ID, name, and so forth, use the **show vlan command**. VTP information, such as mode, domain, and so forth, can be displayed via the **show vtp status** command. Do not panic if the VLAN information and the VTP information are not displayed through **show running-config** when the switch is in VTP server/client mode, as this is a normal behavior. Also ensure that either no password is set between the server and client, or that the password is identically set on both sides.

NOTE: VTP version 2 includes supports for Token Ring LAN switching and VLANs, Unrecognized Type-Length-Value (TLV), Version-Dependent Transparent Mode and Consistency Checks.

Configure, verify, and troubleshoot RSTP operation.

RSTP will assign a port role to the individual ports. A root port provides the best path when the involved switch is forwarding packets to the root switch. A designated port refers to the port through which a designated switch is attached to the network. An alternate port provides an alternate path toward the root switch, while a backup port serves as a backup for the path offered by the designated port. A disabled port has no role at all within the entire operation.

For purpose of the exam, understand the following key points:

- RSTP allows for rapid convergence of the spanning tree. MSTP (Multiple STP) makes use of RSTP for providing rapid convergence, thus enabling multiple VLANs to be grouped into one spanning tree instance.
- Per-VLAN RSTP is not supported.
- For multiple switches to be maintained in the same MST region, they must be equipped with the same VLAN-to-instance mapping. Use spanning-tree mst configuration to enter into the MST configuration mode. Use spanning-tree mode mst to enable MST, which would also automatically enable RSTP.

NOTE: When working with Rapid Spanning Tree Protocol (RSTP), or also known as IEEE 802.1w, you need to know the differences between standard STP and RSTP. With STP (802.1d), there may be lag time to get the topology converged because of the main port roles in which a port may go through – such as blocking, listening, learning and so on. With RSTP, the process has been shortened and made quicker in order to bring a port back up in less than a minute, where with 802.1d, the port could have remained inactive (or unusable) for a period of a minute or more. With RSTP, the two port roles included in the active topology are 'root' and 'designated'.

Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network.

Troubleshooting in general

Use the show commands 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 can 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.

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 identify a router suspected of delivering bad routing information.

Use SHOW IP ROUTE to display the current state of the routing table. If you specify that you want 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.

It is also possible to use the debug commands only during non-peak hours. The debug commands are highly processor intensive. They can slow things down almost to a halt.

Implement basic switch security (including: port security, unassigned ports, trunk access, etc.)

Security is increasingly gaining attention, especially when modern networks are known to have much vulnerability. A penetration test may come to the rescue. It involves the use of various methods for evaluating the security of a computer or a network by simulating an actual attack. The process involves a thorough analysis of weaknesses or vulnerabilities as carried out from the perspective of a serious attacker. Any security issues that are found will then be addressed for considering mitigation or technical solution. This type of assessment is necessary, especially on computer about to be deployed in a hostile environment.

When dealing with switch security, attention is actually focused on layer 2. Why is it necessary to care about layer 2 security? Generally speaking, layer 3 has the primary responsibility of sending data packets from the source network to the destination network using a pre-specified routing method. Because threats from the internet are IP based, filtering at layer 3 is what has to be done to safeguard against these threats. However, once entered into the private network, traffics are processed through switches at layer 2. And in fact there could be threats from *inside* the private network (internal threat that is). Therefore, layer 2 security is a topic that deserves serious attention.

Port security could be the best tool against spoofing attacks. The port security feature of the 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 assigning a single secure MAC address, 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. It is possible to 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.

NOTE: When you want to configure port security, you need to use the **switchport port-security** command. If you want to restrict the amount of users (or connections) to a specific port, you need to add more to the command. In order to restrict a port to a maximum of 10 connections, you need to use the **switchport port-security maximum 10** command.

Chapter 2 - Implement an IP Addressing Scheme and IP Services to Meet Network Requirements in a Medium-Size Enterprise Branch Office Network

Calculate and apply a VLSM IP addressing design to a network.

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 use 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, it is necessary to use a routing protocol that supports it.

NOTE: Note that EIGRP, IS-IS, OSPF and static routes support VLSM, while other routing protocols (such as RIP and IGRP) do not.

The key to VLSM is that it allows for the use different masks for different subnet. For example: With a traditional classful address in the form of 204.15.5.0/27 (host address range 1 to 30, although it is only essential to support 14 hosts), it is possible to use a /28 (255.255.255.240) mask to provide a more precise support of 14 hosts.

NOTE: Variable Length Subnet Masks (VLSMs) are used to give an organization the ability to use more than one subnet mask within the same network address space. This is used to save address space and maximize your address usage to handle growth and future development.

Determine the appropriate classless addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment.

CIDR

When your goal is to implement classless routing, you need to configure your routing protocols to behave properly. You would not want the auto summarization of your routes, therefore if using RIP (version 2 only) and EIGRP, under the routing process, use the no auto-summary command. For the CCNA exam, its important to note that the types of questions you will generally be asked will have 'multiple' concepts you will have to know (and how they interwork together) in order to answer.

With Classless Inter-Domain Routing (CIDR) addressing, 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 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.

NOTE:	Since Class B Internet addresses are in short supply, larger networks are usually granted a contiguous block of Class C addresses. With the traditional way of routing, very large routing tables are in need to cover multiple Class C routes that have to be defined for each network containing more than 254 nodes. Large routing tables are not preferable as they increase the workloads of the routers and thus reduce performance. Supernetting, also known as Classless InterDomain Routing, is defined in RFC 1519 and is referring to the technique that has each of the larger networks represented by a single routing table entry. To achieve this, supernet addressing permits each supernet to be assigned its own netmask. Further information on this topic is covered under the various routing related objectives.

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.

Summarization

Using route summarization can reduce routing table size. The essential skill to master in order to work out route summarization is binary math. Strictly speaking it is not required to do much calculation. The skill to read them, however, is required.

NOTE:	Summarization is typically controlled via the auto-summary command. Note that only classless routing protocols support route summarization. RIP and IGRP do not support route summarization, while RIP V2 does support automatic route summarization.

Binary arithmetic

As a positional notation with a radix of two, the binary numeral system represents numeric values using 0 and 1. A binary number can be represented by any sequence of bits, which in turn may be represented by any mechanism capable of being in two mutually exclusive states.

Counting in binary is similar to counting in the decimal number system. Beginning with a single digit, counting proceeds through each symbol in increasing order. When the symbols for the first digit are exhausted, the next-higher digit to the left is incremented, and counting starts over at 0.

The simplest arithmetic operations in binary are addition and subtraction. Adding two single-digit binary numbers is relatively straight forward:

0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 10

1+ 1 produces the value "10", which is equivalent to the decimal value 2.

Subtraction works similarly. Note that subtracting a positive number is equivalent to adding a negative number of equal absolute value:

0 - 0 = 0
0 - 1 = 1
1 - 0 = 1
1 - 1 = 0

Bitwise logical operations

Sequences of binary bits can be manipulated using Boolean logical operators (we call it bitwise operation). The logical operators AND, OR, XOR and NOT are involved:

- A bitwise OR takes two bit patterns of equal length, and produces another one of the same length by matching up corresponding bits and performing the logical OR operation on each pair of corresponding bits. In each pair, the result is 1 if the first bit is 1 OR the second bit is 1. Otherwise, the result is 0.

- A bitwise exclusive OR takes two bit patterns of equal length and performs the logical XOR operation on each pair of corresponding bits. The result in each position is 1 if the two bits are different, and 0 if they are the same.

- A bitwise AND takes two binary representations of equal length and performs the logical AND on each pair of corresponding bits. In each pair, the result is 1 if the first bit is 1 AND the second bit is 1. Otherwise, the result is 0.

- A bitwise NOT performs logical negation on each bit. 0 digits become 1, and vice versa.

Calculation

When given several networks and asked to come up with the summary address and mask, all that is required is to break the network numbers down into binary strings. Then from left to right, find a line where all the networks no longer have any bit in common (see the example with the first 2 octets in action below):

100 17 = 01100100 00010001

100 18 = 01100100 00010010

100 19 = 01100100 00010011

01100100 000100!!

When converting them back to digits, just ignore those represented by "!", and the result will be a summary network number of 100.16 (for the first 2 octets). The mask in this case would be 11111111 11111100 00000000 00000000 since there are two "!" at the end of the second octet.

Describe the technological requirements for running IPv6 (including: protocols, dual stack, tunneling, etc); Describe IPv6 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.

NOTE: A sequence of 16-bit fields of hex values separated by colons form an IPv6 address. The hex letters in the fields are case insensitive. The address prefix is written in the form of prefix/prefix-length, which is often used for representing the bitwise contiguous blocks of the address space.

For purpose of the exam, know the following:

- The three major types of IPv6 addresses are unicast, anycast, and multicast.
- IPv6 is NEVER truly backward compatible with IPv4 by design. However, network nodes with dual stacks will be equipped with both an IPv4 protocol stack and an IPv6 stack so interoperability can be made possible.
- With the dual stack in place, the same transport protocols of TCP and UDP may run over IPv4 and IPv6. The same applications may also run over both of them.
- Through Tunneling, IPv6 domains that are connected through IPv4 networks may communicate with each other.
- An IPv4-mapped IPv6 address may be used to identify an IPv4-only node to an IPv6 node.
- An IPV6 site-local address is a special type of unicast address that has the prefix FEC0::/10. This kind of addresses can be used to define addressing for an internal site and limit access without relying on any of the globally unique prefixes. In other words, use them as private addresses.
- It is possible to define an IPV6 anycast address, which is basically an address that has been assigned to interfaces of different network nodes. By assigning a unicast address to multiple interfaces, it is, effectively, turned into an anycast address.

NOTE: When studying for the CCNA exam, you will need to review the fundamentals of IPv6 (also known as IPng). There are many new and significant security and service enhancements included with the new version of IP such as newer versions of secure Application layer protocols and encryption possibilities. With IPv4, you work with different types of addresses such as Unicast, Multicast and Broadcast. With IPv6, you still use many of the same addressing methods, as well as the newly developed anycast address. This is used when you need a global unicast address assigned to multiple interfaces on a network device.

6to4 tunnels (sometimes just referred to as ‘6to4’) are a solution that allows you to use IPv6 over an IPv4 network. This configuration is typically configured when you need to have IPv6 packets transmit over your preexisting IPv4 based network. A dual stack simply means that you have two TCP/IP protocol stacks configured on a host, one with IPv4 and one with IPv6. Both solutions can be used to transition with or have a 'dual use' purpose.

Identify and correct common problems associated with IP addressing and host configurations.

Subnet and subnet mask

IP networks can be divided into smaller networks known as subnets. Subnetting refers to the process of dividing a larger network into several smaller subnets for the purposes of extra flexibility, more efficient use of network addresses, and broadcast traffic containment.

NOTE: Most addressing problems are the result of improper subnetting. If subnetting is done correctly, the result should be an error free addressing scheme.

A subnet address can be created by borrowing bits from the host field and designating them as the subnet field. The number of borrowed bits does vary, depending on the subnet mask specified. Do keep in mind that:

- Subnet masks always use the same format and representation technique as the regular IP addresses.
- Subnet masks have binary 1s in all bits specifying the network and subnetwork fields, and binary 0s in all bits specifying the host field.
- Subnet mask bits always come from the left-most bits of the host field.
- The table below shows the binary representation of the subnet masks.

Subnet mask and the binary representations	
Mask	**Binary**
128	10000000
192	11000000
224	11100000
240	11110000
248	11111000
252	11111100
254	11111110

The following tables summarize the key information for each address class. There are 5 columns. the first shows the number of bits borrowed from the host portion, the second shows the subnet mask, the third shows the effective number of subnets created, the fourth shows the number of hosts that can be accommodated per subnet, and the last one shows the number of subnet mask bits.

Class A Host/Subnet Table

1	255.128.0.0	2	8388606	/9
2	255.192.0.0	4	4194302	/10
3	255.224.0.0	8	2097150	/11
4	255.240.0.0	16	1048574	/12
5	255.248.0.0	32	524286	/13
6	255.252.0.0	64	262142	/14
7	255.254.0.0	128	131070	/15
8	255.255.0.0	256	65534	/16
9	255.255.128.0	512	32766	/17
10	255.255.192.0	1024	16382	/18
11	255.255.224.0	2048	8190	/19
12	255.255.240.0	4096	4094	/20
13	255.255.248.0	8192	2046	/21
14	255.255.252.0	16384	1022	/22
15	255.255.254.0	32768	510	/23
16	255.255.255.0	65536	254	/24
17	255.255.255.128	131072	126	/25
18	255.255.255.192	262144	62	/26
19	255.255.255.224	524288	30	/27
20	255.255.255.240	1048576	14	/28
21	255.255.255.248	2097152	6	/29
22	255.255.255.252	4194304	2	/30
23	255.255.255.254	8388608	2*	/31

Class B Host/Subnet Table				
1	255.255.128.0	2	32766	/17
2	255.255.192.0	4	16382	/18
3	255.255.224.0	8	8190	/19
4	255.255.240.0	16	4094	/20
5	255.255.248.0	32	2046	/21
6	255.255.252.0	64	1022	/22
7	255.255.254.0	128	510	/23
8	255.255.255.0	256	254	/24
9	255.255.255.128	512	126	/25
10	255.255.255.192	1024	62	/26
11	255.255.255.224	2048	30	/27
12	255.255.255.240	4096	14	/28
13	255.255.255.248	8192	6	/29
14	255.255.255.252	16384	2	/30
15	255.255.255.254	32768	2*	/31

Class C Host/Subnet Table				
1		255.255.255.128	2	126
	/25			
2		255.255.255.192	4	62
	/26			
3		255.255.255.224	8	30
	/27			
4		255.255.255.240	16	14
	/28			
5		255.255.255.248	32	6
	/29			
6		255.255.255.252	64	2
	/30			
7		255.255.255.254	128	2*
	/31			

NOTE: For the CCNA exam, there will be no escaping the need to master how to subnet the IPv4 address space. If you do not know the basics of subnetting and have a good concept of how to derive a subnet mask, you will surely fail the exam. Almost every other question on the exam tests your knowledge of TCP/IP and IP subnetting.

For the exam, the above table can help you to get through. If you can memorize the basic subnets for class A, B and C networks, then you will be able to take the exam. You will need to know how many hosts and networks you can get from taking bits from either grouping.

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**.
- 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.

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.

If the host fails to communicate with hosts on another subnet, chance is that the default gateway setting is wrong. From the host perspective a gateway is a node on a LAN that serves as an entrance (or exit) to another network. When opening up a Command Prompt on Windows 2000 or XP Professional desktop and type in ipconfig, a Default Gateway entry in the output will appear. The gateway address should be the IP address of the router's interface to the subnet.

```
Connection-specific DNS Suffix  . :
IP Address. . . . . . . . . . . . : 192.168.2.100
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.2.1
```

Chapter 3 - Configure and Troubleshoot Basic Operation and Routing on Cisco Devices

Compare and contrast methods of routing and routing protocols.

Routing overview

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".

NOTE: 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. 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.

To enable dynamic routing between Cisco routers, deploy at least one of the following routing protocols inside the network:

- 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 working with smaller network and trying to avoid a 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, link-state protocol is the ideal choice, as long as the complexity of the task is practical.

NOTE: 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.

Configure, verify, and troubleshoot OSPF.

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, limit the explosion of link state updates 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.

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 the network environment, carefully coordinate the configurations of all the running routers.

To enable OSPF in the 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 can be used to enable OSPF routing and enter into the router configuration mode. Remember to supply a process-id for this command. 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.

NOTE: To troubleshoot OSPF effectively, acquire the output of the following commands: show ip ospf neighbor, show ip ospf neighbor, and/or show tech-support.

When attempting to solve a problem with OSPF, you may find it handy to use the ip ospf debug packet command. This will allow you to analyze each packet transmitted and capture so that you can find problems and resolve them.

The **debug ip ospf packet** command is useful in finding out packet level information. The debug ip ospf packet command produces one set of information for each packet received. The output varies slightly depending on which authentication (such as MD5) is used. The following output is from an OSPF packet level debug:

OSPF: rcv. v:2 t:1 l:48 rid:10.1.100.12

aid:0.0.0.0 chk:0 aut:2 keyid:1 seq:0x0

As you can see from the output, the fields are all shortened with numbers and lettered abbreviations so decode the debug output, you can use the following chart.

v:OSPF version
t:OSPF packet type Packet types:
1:Hello
2:Data description
3:Link state request
4:Link state update
5:Link state acknowledgment
l:OSPF packet length in bytes
rid:OSPF router ID
aid:OSPF area ID
chk:OSPF checksum
aut:OSPF authentication type Authentication types:
0:No authentication
1:Simple password
2:MD5
keyed:MD5 key ID
seq:Sequence number

Configure, verify, and troubleshoot EIGRP.

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.

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.

NOTE: When you use EIGRP, you have to understand how it interoperates with IP. For example, if you want to summarize your updates, you can use the **auto-summary** command. If you do not want the updates summarized and you want to include the subnet mask details within the update, then you can use **no auto-summary** command under the configured routing process. Route summarization when configured correctly, can reduce the amount of routing information in the routing tables to keep the routing process more efficient.

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.

NOTE: To troubleshoot EIGRP effectively, acquire the output of the following commands: show interfaces serial , show ip eigrp neighbors , show tech-support , and/or show ip eigrp topology.

Verify configuration and connectivity using ping, traceroute, and telnet or SSH.

Troubleshooting with ping and traceroute

A bottom up approach requires to first start at the physical layer. Possible problems at the physical layer can include:

- Incorrect configuration
- Faulty or 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 it is not possible 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 going to all the next hops and testing connectivity from there. **PING** and **extended PING** is primarily used to conduct such kind of testing.

Where **PING** can be used to verify connectivity between network devices, the **TRACEROUTE** command can help to discover the paths packets take to a remote destination and determine if

routing breaks down at a particular point, through 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 the attention to where the actual problem is occurring.

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 wanting to discover the correspondences between all network addresses (including non-IP addresses) and the LAN hardware addresses, use the SHOW ARP command instead.

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 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.

NOTE: To properly troubleshoot adding problems, use ping and traceroute. Ping is almost always your best friend. Refer to Objective 4 of the next chapter for further in-depth information.

Troubleshoot routing implementation issues.

Using 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 able to be 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---

SHOW IP PROTOCOLS can be used 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 identify a router suspected of delivering bad routing information.

SHOW IP ROUTE can be used to display the current state of the routing table. If specifying that you want 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.

NOTE:	If a router cannot find a valid startup configuration file in NVRAM during router its startup routine, then it will enter what is called 'setup mode'. Setup mode is interactive. Setup mode provides a menu driven help system to guide you through the process of creating an initial configuration file whether the system is new, or if you have removed (erased) the current startup configuration file from NVRAM.

Split horizon and Holddown Timers

The RIP routing protocol when configured on the routers in your network will send out routing update messages to adjacent neighbors at regular internals as well as for topology changes. When updates are sent to adjacent neighbors, each router analyzes the update and makes any changes to its already established route table. When routes are updated, the metric value for that path is incremented by 1. Any router running RIP will keep the best path stored in their tables. Any route with the lowest metric value will be the best route considered. RIP is kept stable by a number of services such as holddown timers and split horizon. These mechanisms prevent incorrect routing information from being propagated throughout your network. In situations such as this where you are monitoring the operation of RIP, it's helpful to remember how RIP operates. In this case, if a route is in holddown and an update is received with a good metric and a viable path, the holddown will be removed and the route will be marked as accessible in the route table

Holddown timers and appropriate settings when configured correctly are in place to ensure that regular update messages aren't tainted with incorrect information. For example, when a router drops off the network, its adjacent neighbors will detect the drop and then try to calculate new tables. When the holddown timer is set, routers are told to hold down any changes to the topology so that routes can be correctly placed in the routers tables as well as to achieve a quicker and more accurate convergence. For RIP, the holddown timer default setting is 180 seconds

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.

Troubleshoot physical problems

If the problem could be with network media, the following tools may be useful:

- Volt-ohm meters and digital multimeters can be used 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.

Verify router hardware and software operation using SHOW & DEBUG commands.

The SHOW commands again

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 can be 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.

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.

Use the DEBUG ALL command 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.

NOTE: **debug ip rip** is the command you can use to display information on Routing Information Protocol (RIP) routing transactions. It provides useful information that can help you troubleshoot routing problems on your network when you suspect that the routing updates aren't getting to their intended interfaces. In the following example, you can see how the debug command shows you updates on configured interfaces

Router resources

Sometimes the router may appear sluggish or may not respond at all, which is quite likely a hardware resource issue. These can be done 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. At least 5 percent of total router memory should be free. If this is not the case, use **show process memory** to identify the process that is eating up the router memory.

- To determine if the 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 use **show process cpu** to find out which processes are running and how much CPU they are using.

Implement basic router 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 mode you are currently in. When logging in, begin 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. Use the ENABLE SECRET command 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 that 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 IOS releases, configure Message Digest 5 (MD5) encryption for the passwords. MD5 is a one-way hash function. It makes reversal of an encrypted password almost entirely impossible, therefore is capable of providing very strong encryption protection. To use this feature, rely on the username secret command to specify a username and its associated MD5-encrypted secret.

Chapter 4 - Implement, Verify, and Troubleshoot NAT and ACLs in a Medium-Size Enterprise Branch Office Network

Describe the purpose and types of access control lists.

Cisco router provides 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 a minimum, configure ACLs on the border routers to provide a basic buffer from the outside network or from a less controlled area of the network into a more sensitive area of the private network. On these routers, configure ACLs for each network protocol configured on the router interfaces. It is ideal to have both the inbound traffic and the outbound traffic filtered on an interface if the performance tradeoff is justified.

Do keep in mind that router ACLs are never sophisticated enough for protecting the network against intentional hacking attacks. If the network is a popular attack target, consider installing a full-blown firewall instead.

NOTE: Access control lists (also known as ACLs) can be used to restrict or permit access to a Cisco device. You can use ACLs to control the flow of traffic as well as many other purposes. ACLs can be added to interfaces, vty access and so on. For the CCNA exam, you will be given situational questions that test your ability to quickly use IP addresses within standard and extended ACLs based on IPv4.

Configure and apply access control lists based on network filtering requirements.
ACLs must be defined on a per-protocol basis. It is necessary to define ACLs for every protocol enabled on an interface, if the goal is to control traffic flow for that protocol. At present the following protocols are supported:

- Apollo Domain
- IP
- IPX
- ISO CLNS
- NetBIOS IPX
- Source-route bridging NetBIOS

As ACLs are created, they need to be assigned a number (or a name) to each list. Each type of list is limited to an assigned range of numbers. The table below lists all the valid ACL number ranges:

Protocol	Range
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
Ethernet type code	200-299
Ethernet address	700-799
Transparent bridging (protocol type)	200-299
Transparent bridging (vendor code)	700-799
Extended transparent bridging	1100-1199
DECnet and extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
AppleTalk	600-699
Source-route bridging (protocol type)	200-299
Source-route bridging (vendor code)	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099
Standard VINES	1-100
Extended VINES	101-200
Simple VINES	201-300

NOTE: For the CCNA exam you need to know how to deploy 'extended' ACLs. For the CCNA exam, you will need to know how to deploy different types of ACLs other than standard based. Most commonly used are IPv4 standard and extended access lists.

IP Standard
1 to 99
1300 to 1399

IP Extended
100 to 199
2000 to 2699

Configure and apply an access control list to limit telnet and SSH access to the router.

Access list elements

As previously stated, create access lists for each protocol that needs to be filtered, on a per router interface. For some protocols, it may be necessary to create one access list to filter inbound traffic and another one to filter outbound traffic.

To create an access list, specify the following elements:

- 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 a number must identify access lists of other protocols. Some protocols can be identified by either a name or a number. The numbers are the only requirement for the exam, however.

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

NOTE: Controlling outbound access on vty lines can be tricky. Most times, ACLs are applied to interfaces and when you do, there is a different command for it. For the exam, you need to remember the difference between securing a vty interface and an Ethernet interface. The following example defines an access list that denies connections to

networks other than network 171.16.0.0 on the vty port. The following example is the configuring of the vty lines 0 4 for the access list to take affect on the routers vty lines for one of two core routers.

```
core_rtr1(config)#access-list 11 permit 172.16.0.0 0.0.255.255
core_rtr1(config)#line vty 0 4
core_rtr1(config-line)#access-class 11 out
```

Most times, ACLs are applied to interfaces for security. For the exam, you need to remember the difference between securing a vty interface and an Ethernet interface. The following example is the configuring of an interface on a router (ethernet1) with an access list that allows http based traffic to a web server with an IP address of 172.16.2.1 only and deny all other IP based traffic.

```
core_rtr1(config)#access-list 101 permit tcp any host 172.16.2.1 eq 80
core_rtr1(config)#access-list 101 deny ip any any
core_rtr1(config)#interface ethernet1
core_rtr1(config-if)#ip access-group 101 in
```

IP access lists

It is possible to have 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 allows for the permitting or denying of traffic from specific IP addresses, regardless of the destination of the packet and the ports involved. An example:

```
access-list 10 permit 192.168.1.0 0.0.0.255
```

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. They also allow for the specifying of different types of protocols for more granular control of traffic flows. An example:

```
access-list 101 permit tcp 111.111.2.0 0.0.0.255 any eq 80   ( <-  80 means "port 80")
```

NOTE: Rely on extended access lists to filter telnet and SSH traffics. The concerned port numbers are tcp 22 and 23. A SSH connection looks highly similar to a telnet connection but SSH runs on tcp port 22 instead of port 23.

Verify and monitor ACLs in a network environment.

ACL Statements

For a single access list, it is possible to define multiple criteria in multiple, separate access list statements. In theory, it is almost possible to have as many criteria statements as desired, but this is subject to the memory capacity of the router. From a practical standpoint, having too many statements makes them harder to manage.

At the end of every access list is an implied "deny all traffic" criteria statement (something which looks like *access-list 10 deny any*). If a packet does not match any of the criteria statements, this statement will block the packet.

Basic ACL commands

To define a standard IP access list, it is possible to use the standard version of the **access-list** command in global configuration mode. An example:

> **access-list** 11 permit 192.168.2.0 0.0.0.255

The above list (numbered 11) allows traffic from all addresses in the range 192.168.2.0 to 192.168.2.255.

To remove the access list, use the no form of the same command.

The **show access-lists** EXEC command can be used to display the contents of all access lists. For example, the below command displays the content of the access list 11.

> **show access-list** 11

Use the **show ip access-list** EXEC command to display the contents of a particular access list.

Troubleshoot ACL implementation issues.

Do understand that it is impossible to reorder or delete criteria statements on a router. That is, if there is a need to edit a small part of a statement, the entire list will have to be deleted and re-entered again. That is why it may be better off to create all access list statements on a TFTP server, and then download them to the router.

To use a TFTP server for this purpose, first create the access list statements using a text editor and save them in ASCII format to a TFTP server that is accessible on the network. Then, from the router, use the **copy tftp:***file_id* **system:running-config** command to copy the access list to the router. Finally, use the **copy system:running-config nvram:startup-config** command to save the access list to the router's NVRAM.

The show ip access-lists can always be used to find out what IP access lists are applied and how they are doing. If they have denied too much traffic, it may be necessary to reconfigure the lists. The bottom line is, if they have denied too much traffic, something is obviously being too restrictive, and they need reconfiguring. There has to be a tradeoff between security and usability. Remember to make the appropriate judgment accordingly.

It is also possible to further configure access list logging via ip access-list logging. Warning: use the debug command ONLY when the router is not under heavy load, or the router processor will be over taxed. Also note that access list debugging is way more processor intensive than simple logging. So don't do it until everyone on the network is off-work. To remove a list that is no longer useful, consider having a "no" placed right in front of the access-group command.

NOTE: It is very important to understand that each new criteria statement that is entered is appended to the end of the access list statements. Therefore, the order of access list statements is important - IOS tests each packet against each criteria statement in the order in which the statements were created. After a match is found, no more criteria statements are checked.

Explain the basic operation of NAT.

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 an internal address to be substituted by a fixed external IP address, is useful for servers that require fixed IP addresses.

Static NAT is a form of NAT that maps one unregistered private IP v4 address to one registered public IP v4 address. Dynamic NAT is a form of NAT that generates these mappings from a 'pool' of addresses. Static NAT is a form of NAT that maps one unregistered private IP v4 address to one registered public IP v4 address. When you configure a static mapping from one IP address to another, you are creating a permanent translation between two hosts. Depending on the verbiage used (such as inside, or outside), you can translate inside to outside and vice versa. The following commands shows you an example of the ip nat inside source static command mapping two IP address together.

ip nat inside source static 10.1.1.1 192.168.1.1

When deploying NAT, you need to configure the pool if you choose to draw from a pool when translating. NAT can be configured dynamically. In this example, you needed to know the command in which to configure a pool. For the CCNA exam, you will need to know how to configure a variety of NAT and PAT configurations so be sure to make sure you understand the command set for deploying translation. In this example, we are creating a NAT pool (10.1.1.1 – 10.1.1.254) that defines Outside Local addresses to be used for translation.

ip nat pool POOLNAME 10.1.1.1 10.1.1.254 netmask 255.255.255.0

NOTE:	For the CCNA exam, you will need to know how to configure most aspects of NAT manually as well as test after you troubleshoot your work. Make sure that you study the inner workings of NAT very carefully when preparing for your exam.

Configure Network Address Translation for given network requirements using CLI.

To configure an inside NAT interface, use the interface configuration sub-command "ip nat inside". To configure an outside NAT interface, use "ip nat outside" instead. To disable NAT, use "no ip nat {inside|outside}".

At any time, the translation table with the use of "**show ip nat translations**".

NOTE:	The key to successful implementation is the clear understanding of the difference between "inside" and "outside". An "outside" network is one that is reachable from hosts outside of the network, such as the Internet. An "inside" network is one that is only reachable from an administrative connection that is inside the private network.

The command **ip nat inside** will configure an interface to use NAT. This would be considered the 'inside' interface when further configuring network address translation. The command **ip nat outside** will configure an interface to use NAT also, but this interface will be considered the 'outside' interface when further configuring NAT statements.

Pay attention to the following two points when configuring NAT:

- The keyword overload used in the ip nat statement allows NAT to translate multiple inside devices to the single address in the pool.
- Do not configure access lists referenced by NAT commands with "permit any" because it will consume too many router resources.

For the exam, you need to be familiar with the fundamentals of assigning addressing within NAT. An Inside global address is a legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world. You should be familiar with all of the technical details of NAT such as placement of addresses, naming interfaces and assigning lists.

- Local address: A local address is an address that is configured for an inside segment of the network
- Global address: A global address is the address that is configured for an outside segment of the network
- Inside local address: The IP address assigned to a host on the inside network. This is the address configured as a parameter of the computer OS or received via dynamic address allocation protocols such as DHCP. The address is likely not a legitimate IP address assigned by a service provider.
- Inside global address: A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world
- Outside local address: The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside
- Outside global address: The IP address assigned to a host on the outside network by the host owner. The address is allocated from a globally routable address or network space

Troubleshoot NAT implementation issues.

NAT is not without drawbacks and restrictions. It is said that the dynamic allocation (of IP addresses, in the form of NAT) requires state information that may not always be available. This is especially true for UDP traffic, which offers almost no mechanism (at the packet header level) for determining if a packet is part of an ongoing communication session.

Also, since NAT has to base translations on information contained in the packet headers, it may not support certain protocols that hide those information in somewhere else. For example, NAT may not fully support NAT sensitive protocols such as Kerberos, X-Windows, remote shell, and SIP.

Other potential restrictions are:

- NAT may interfere with some encryption systems as NAT itself is tampering with the packets.
- NAT may also interfere with logging as logging information is often provided AFTER a translation.

NOTE: NAT is highly processor and memory intensive. Each NAT table entry costs approx 160 bytes of memory, so the scalability of the NAT implementation really depends on the router hardware platform and the corresponding performance specifications.

Chapter 5 - Implement and Verify WAN Links

Configure and verify Frame Relay on Cisco routers.

Frame relay is a telecommunication service designed for transmitting intermittent data traffic between LANs and between end-points in a WAN. It works by putting data in a variable-size frame and leaves any necessary retransmission up to the end-points, thus capable of speeding up overall data transmission. Frame relay allows an enterprise to select a level of service quality (QoS) by prioritizing frames, thus making it an ideal choice for connecting LANs with major backbones as well as on public WANs with dedicated connections during the transmission period. Note that it is still a X.25 like packet switching technology and is therefore not suitable for steady streams of voice or video transmission.

NOTE: Although Frame Relay is already deemed a legacy protocol, its still in use and you must know how to support it not only for the CCNA exam, but also within production networks. For the CCNA exam, there are many Frame Relay related questions, especially those revolving around how specific routing protocols operate over this specific type of network. Make sure you cover these areas carefully before taking the exam. Make sure you know how protocols such as RIP, IGRP, EIGRP and OSPF operate over Frame Relay WANs.

Frame Relay can be used as an interface to either a publicly available carrier-provided service or to a network of privately owned equipment. A public Frame Relay service is deployed by having Frame Relay switching equipment configured in the central offices of a carrier service provider. Users are accordingly relieved from the overheads necessary for administering and maintaining the network equipment and service.

NOTE: Local Management Interface (LMI) is a signaling standard created to use between routers on a Frame Relay network. LMI will signal from the router to the Frame Relay switch. LMI is responsible for managing the connection and maintaining status between network devices. When a connection is made between a router and a Frame Switch, a PVC is generated and LMI runs within the PVC. The three types of LMI that Cisco devices can support are ANSI, Cisco and Q.933A.

The basic steps for enabling Frame Relay on an internetwork include:

1. Enable Frame Relay Encapsulation

To enable Frame Relay encapsulation at the interface level, specify the serial interface via the interface serial number command. To specify the encapsulation method to use, invoke the encapsulation frame-relay [ietf] command.

2. Configure either Dynamic or Static Address Mapping

To define address mapping use the frame-relay map protocol protocol-address dlci [broadcast] [ietf] [cisco] command. Note that the three supported protocols are ip, AppleTalk and ipx.

3. Configure the Local Management Interface (LMI)

To specify the LMI type, use frame-relay lmi-type {ansi | cisco | q933a}

Traffic can be separated among different data-link connection identifiers (DLCIs) based on protocol type. To do so, assign specific protocols to specific DLCIs by specifying static mapping on a per virtual interface basis or by defining only specific types of encapsulations for specific virtual interfaces.

NOTE: When you need to configure Frame Relay, you will need to know how IP addresses are mapped to corresponding DLCI numbers. Inverse ARP is a protocol used for the purpose of obtaining Layer 3 addresses from remote stations as per their Layer 2 addressing information (DLCI). Inverse ARP is commonly and primarily used in Frame Relay (and ATM) based WANs. A data link connection identifier (DLCI) is a number used and attached to frame relay data frames in order to tell the network how to route the destination data.

When you view the mappings, you can see that a specific circuit may be in an 'inactive' state. For the CCNA exam, you will need to know how to view Frame Relay mappings and determine specific problems. Make sure that you understand how to troubleshoot common Frame Relay problems, specifically with Frame Relay circuit mappings.

Troubleshoot WAN implementation issues.

The output of the **show interfaces serial** EXEC command displays information specific to serial interfaces that are commonly used for WAN communication. It is possible to identify possible problem states via the interface status line of this command.

An interface problem is usually due to faulty/incorrect cabling or hardware failure on the local side. In fact, it is a good idea to regularly verify all cabling. Always ensure that the cable is attached to the correct interface, the correct CSU/DSU, and the correct telephone company network termination point. The **show controllers** EXEC command can be used to determine which cable is attached to which interface.

A faulty CSU/DSU may also contribute to the interface problem. A failed CSU/DSU often fails to provide the router interface with the necessary carrier detect signal.

If the interface is up but the line protocol is down, it is necessary to determine if this is a problem on the telephone company side/remote side. This can be done by putting the modem, CSU, or DSU in local loopback mode and use the **show interfaces serial** command to determine whether the line protocol comes up. If the line protocol comes up, it has to be a telephone company problem or a problem on the remote router. On the other hand, if the line protocol does not come up even in local loopback mode and if the output of the **debug serial interface** EXEC command reveals that the keepalive counter is not incrementing, the router hardware may be faulty and may require replacement.

The output of the various **debug** privileged EXEC commands displays diagnostic information relating to protocol status and network activity of different sorts. However, since debugging output is assigned high priority in the CPU process, it can render the system unusable. Therefore, use the **debug** commands sparingly – use them only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Do so only during periods of low network traffic.

For the CCNA exam, make sure you review how distance vector protocols operate over Frame Relay WANs. Distance-vector routing protocols use the split horizon rule which stops a router from advertising a route back out the interface from which it was learned. Split horizon is one of the methods used to prevent routing loops due to the slow convergence times of distance-vector routing protocols. The **ip split horizon** command enabled split horizon. The **no ip split-horizon** command will disable split horizon on the interfaces that are connecting within the core.

Describe VPN technology (including: importance, benefits, role, impact, components).

VPN is a private network that uses the Internet to connect remote sites or users together. 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

NOTE: Different types of VPN tunnel require different configuration tasks and commands. GRE (Generic Routing Encapsulation) is a tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels for creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. PPTP

(Point to Point Tunnel Protocol) enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across IP networks. L2F (Layer 2 Forwarding) is a protocol that supports the creation of secure virtual private dial-up networks over the Internet. L2TP (Layer Two Tunneling Protocol) combines the best features of Cisco's Layer 2 Forwarding (L2F) and Microsoft's PPTP.

With Cisco VPN devices in place, the use of IPSec becomes quite prevalent. IPSec is a set of protocols for supporting secure exchange of packets at the IP layer. It has two encryption modes: Transport and Tunnel. Transport mode encrypts only the payload of each packet, while Tunnel mode encrypts both the header and the payload.

NOTE:

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 needs to be 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, configure static NAT translations for IPSec to work properly.

Configure and very PPP connection between Cisco routers.

The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol (TCP/IP, IPX/SPX, AppleTalk) datagram's over point-to-point WAN links. When working with PPP, you need to understand how the protocols that work within PPP operate, primarily LCP and NCP. For the exam, you will need to understand the fundamentals of PPP and how to configure and secure it. The Link Control Protocol (LCP) handles many connection establishment options such as encapsulation format. LCP will control the link connection and then terminate it once completed. The Network Control Protocol (NCP) phase in the PPP link connection process will create the different network layer protocol establishment for each routed protocol in use. PPP supports routed protocol such as IP, IPX or AppleTalk. IP Control Protocol (IPCP) messages are sent to set up connection options for each routed protocol in use.

The most common WAN connection method is the telephone modem, which is used to convert the digital data output from the computer into an analog type signal that can be conveyed over the telephone lines, and, in the reverse direction, convert the analog signal received over the telephone lines into digital data that the computer can read. PPP is the choice of encapsulation protocol when modems are in use for communication.

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).

NOTE:

For the exam you will need to know how to encapsulate an interface with PPP.

Use the command **encapsulation ppp** to enable PPP encapsulation.

For the exam you will need to know how to configure PPP authentication. The Point to Point Protocol (PPP) is a WAN based protocol that is used encapsulating, securing and/or transporting multi-protocol data over P2P links. PPP functions at the data link layer of the OSI model. PPP authentication is delivered through other protocols such as CHAP, PAP and EAP. By default, a router will use its hostname to identify itself to its peer router.

Use **ppp authentication {chap | pap}** to configure the use of either CHAP or PAP authentication.

Asynchronous interfaces correspond to physical terminal (TTY) lines. It is also possible to enter commands in asynchronous interface mode to configure protocol-specific parameters for asynchronous interfaces. Also, it is possible to enter commands 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 to configure 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 when dealing with the configuration of more complicated WAN links.

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.