Cisco Certified Network Associate (CCNA) key points

This is my personal summary of what I believe to be the key points of needed to pass Cisco's CCNA composite test. I have no special insight into the test (other than years of teaching the course material.) This summary is not endorsed by ANYONE. This summary represents a minimum base of knowledge for the CCNA. You should know MORE than this before taking the test!

This material is NOT necessarily in the same order as the course material!

Remember that the CCNA is a test of skill as well knowledge. Make sure that you know ALL of the facts listed here and are able to configure ALL of the applications listed here.

Module Self Check Questions

At the end of each module are a series of "Module Self-Check" questions and an answer key. Make sure that you can correctly answer each of these questions!

Network Components

You should be able to contrast a switch, router and computer. For the CCNA test comparisons between computers, routers and switches should be viewed as comparisons between personal computers, 2800 routers and 2960 switches. Routers operate at OSI Layer 3, switches at OSI Layer 2 and hubs operate at OSI Layer 1. You should also know the Cisco symbols of these devices.

Units of measure

Digital: bit **b** (0 or 1), Byte **B** (8 bit), Kilobyte **KB** (1000 bytes), Megabyte **MB** (1,000,000 bytes), Gigabyte **GB** (1,000,000,000 bytes) Terabyte **TB** (1,000,000,000,000 bytes).

Frequency: Hertz **Hz** (cycles per second), Kilohertz **KHz** (1000 cycles per second, Megahertz **MHz** (1,000,000 cycles per second), Gigahertz **GHz** (1,000,000,000 cycles per second), Terahertz **THz** (1,000,000,000,000).

Network Models

Know the **7 Layer OSI model** – Use my seven layer OSI 7 Layer song to memorize this.

Know the **TCP/IP 4 layer model** (Network access, Internet, Transport, Application) and how these layers map to the OSI 7 layer model.

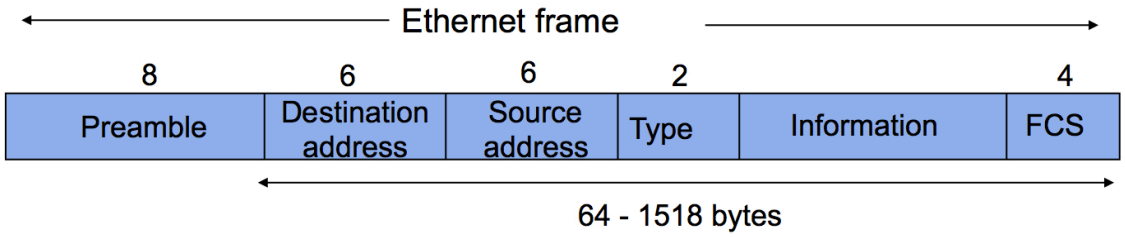
Ethernet

Describe and recognize the structure of a MAC address (**3 bytes OUI** and **3 bytes of unique serial number**).

Describe the **CSMA/CD algorithm**. (When a device wants to transmit on a network, it checks to see if the network is idle (senses the carrier). If it is not, it waits until the network is idle before transmission can begin. If two devices transmit on the line at the same time a collision occurs. Once a collision is detected, both devices back off and each wait a random amount of time before retrying.)

Know the **broadcast address** of Ethernet (ff:ff:ff:ff:ff:ff)

Know the structure of the IEEE **802.3 frame**.

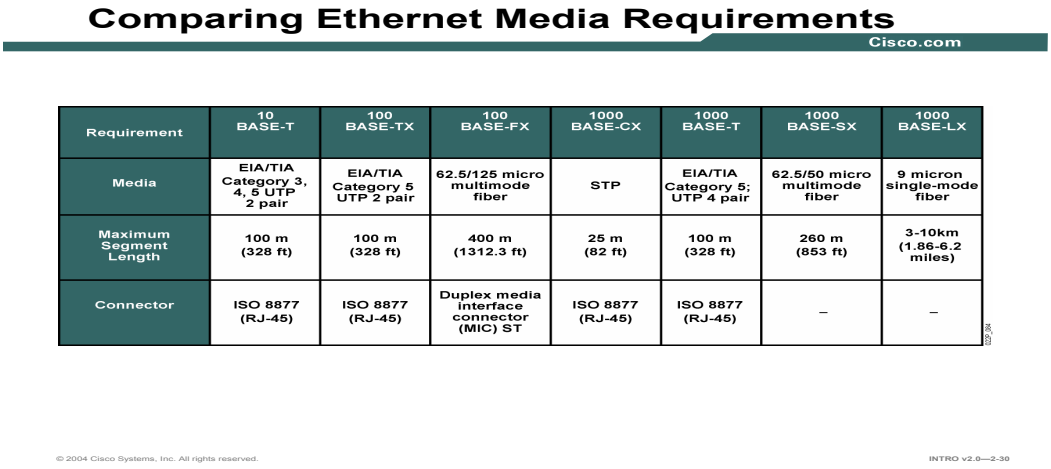


Understand straight through and crossover cables.

For the purposes of cabling, there are two categories of devices those with normal ports and those with crossover ports. PC's, servers and routers have normal ports. Hubs, repeaters and switches have crossover ports. To connect devices from different categories use a straight through cable. To connect two devices from the same category use a crossover cable. **Crossover cables** for 10BASET and 100BASET have pin 1 connected to pin 3, and pin 2 is connected to pin 6

MAC addresses on a switch are stored in **Content Addressable Memory (CAM)**. CAM is also known as a MAC address table. On a Cisco switch dynamically learned MAC Addresses are maintained in the CAM for 300 seconds.

Know the nomenclature, media type and maximum segment length of various Ethernet standards and media.



Comparing Ethernet Media Requirements

Cisco.com

Requirement	10 BASE-T	100 BASE-TX	100 BASE-FX	1000 BASE-CX	1000 BASE-T	1000 BASE-SX	1000 BASE-LX
Media	EIA/TIA Category 3, 4, 5 UTP 2 pair	EIA/TIA Category 5 UTP 2 pair	62.5/125 micro multimode fiber	STP	EIA/TIA Category 5; UTP 4 pair	62.5/50 micro multimode fiber	9 micron single-mode fiber
Maximum Segment Length	100 m (328 ft)	100 m (328 ft)	400 m (1312.3 ft)	25 m (82 ft)	100 m (328 ft)	260 m (853 ft)	3-10km (1.86-6.2 miles)
Connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Duplex media interface connector (MIC) ST	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	–	–

Know the physical wiring layout (topology) for a bus and a star

Understand the following switch concepts:

Collision Domains – a collision domain is a single CSMA/CD network in which there will be a collision if two computers transmit at the same time.

Broadcast Domains – a broadcast domain is a LAN in which any devices attached to the LAN can transmit frames to any other device because the medium is a shared. Broadcast domains are normally delimited by routers.

Switches learn the location of devices remembering the Source MAC addresses of an Ethernet frame as it enters the switch.

Switches flood Ethernet frames with unknown addresses to all ports.

Switches forward Ethernet frames with known addresses to the destination port only.

Filtering is when switches do not forward Ethernet frames with known addresses to ports other than destination port.

Distinguish between the three types of Mac addresses: **unicast, broadcast and multicasts**. A unicast address is addressed to one specific host, a broadcast is addressed to all hosts and a multicast is addressed to a subset of hosts.

A Switched Virtual Interface (SVI) is a Layer 3 Interface on a switch. A switch is a Layer 2 device and has no interaction with Layer 3 (including IP). A Cisco switch is allowed one SVI that is used as a management interface. A Multi-Layer switch can have multiple SVI's and route between them.

IOS Commands

Know these IOS modes:

Prompt for user mode = >

Prompt for privileged mode = #

Prompt for Global configuration mode = **(config)#**

Prompt for interface configuration mode = **(config-if)#**

Prompt for router configuration mode = **(config-router)#**

Prompt for line configuration mode = **(config-line)#**

Know these editing commands:

ctrl-a moves cursor to the beginning of a line
ctrl-e moves the cursor to the end of a line
esc-b moves cursor back one word
esc-f moves cursor forward one word
ctrl-z is the equivalent of return
ctrl-p is the equivalent of up arrow
ctrl-n is the equivalent of down arrow

Switch Related IOS Commands

Master these commands:

Change the name of a switch to NEWNAME **(config)#hostname NEWNAME**

Configure a port for full duplex vs. half duplex
(config-if)#duplex {auto/full/half}

Use **#show interface** to see duplex settings

Set a static mac address
(config)# mac-address-table static 0004.5600.67ab vlan1 int fa0/2

Show the mac table:
#show mac-address-table

Configure default gateway

(config)# ip default-gateway (ip address)

Configure a management vlan

(config)# interface vlan1
(config-if)# ip address (address) (mask)

A MAC flood attack overloads the MAC Address table causing the switch to act like a hub. The port security max feature will prevent this.

Configure port security

(config)#interface fastethernet0/1
(config-if)#switchport mode access
(config-if)#switchport port-security
(config-if)#switchport port-security max 1
(config-if)#switchport port-security violation (protect/rest/shutdown)
(config-if)#switchport port-security mac-address sticky

#show port-security displays ports configured with port security and security action associated with each port.

#show port-security address displays the mac address for each secure port.

Understand that there are **5 sources** of configuration information: Console port, AUX port, VTY, external file storage (TFTP, FTP, etc), Web Based (CiscoCP, SDM, etc.)

Be aware that there are two copies of the configuration file: the running-config, which is stored in the RAM and the startup-config, which is stored in the NVRAM.

Understand that changes to the running-config file are made permanent with the copy running-config startup-config command.

Be aware that the copy command has the following format**: copy *source destination***

Identify the following as characteristics of a switch: high port density, large frame buffers, support for a mixture of port speeds, fast internal switching and low cost per port

Cisco IOS supports: TFTP, FTP, SFTP, RCP, SCP and HTTP for file transfers

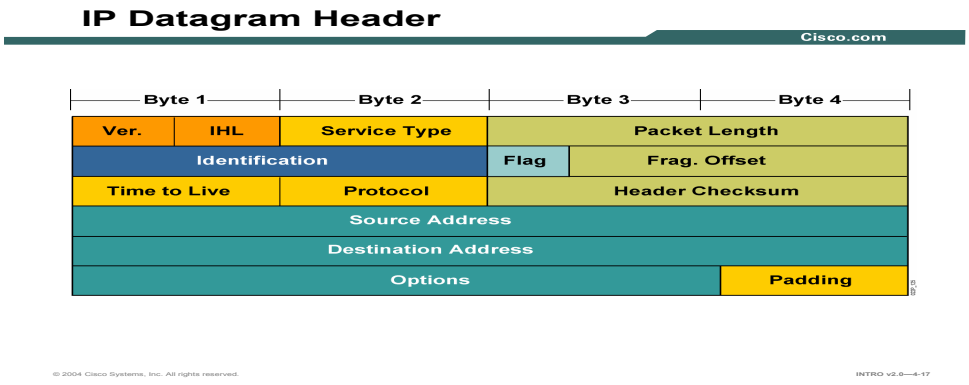
Define the following terms that are associated with the show interface status command:

Runt (a packet which is discarded because it is smaller than 64 bytes)
Giant (a package which is discarded because it is larger than 1518 bytes)
CRC (the total number of errors)

Understand that Fiber optic cable provides higher speeds, longer distances, more reliability and less noise than twisted-pair. However, it is significantly more expensive.

Know that single mode fiber optic cable uses lasers as a light source and multimode fiber uses inexpensive LEDs as a light source.

Know the IP v4 header fields:



The **Version** nibble identifies IPv4 or IPv6.

TOS Type of Service field is how the datagram should be used to be foe QoS, (e.g. delay, precedence, reliability). This TOS field is now called the Differential Services Code Point (DSCP).

TTL (Time To Live) - decrements by one at each router

Protocol – identifies the Layer 3 protocol being carried by IP, common protocols include: 6 (TCP), 17 (UDP), 1 (ICMP)

Source & Destination addresses are 32 bit hierarchical addresses

Understand the following IP related applications:

ICMP messages are delivered in IP packets and are used for out-of-band messages related to network operation and problems. Since ICMP is delivered by IP, ICMP packet delivery is unreliable.

Ping is a program used to test internet connectivity it was created in 1983 by a US government engineer named Mike Muuss. Ping uses the Internet Control Message Protocol (ICMP) Echo request and Echo reply functions which are detailed in RFC 792. A small packet is sent through the network to a particular IP address using the Echo request function. The receiving host responds with an Echo reply packet.

Traceroute sends out a packet to the destination with a TTL value of 1. The packet goes through the first hop and dies, causing the first router to return an ICMP Time To Live exceeded message which reveals ip address of that router.

Traceroute then sends another packet with a TTL value of 2. When it reaches the first hop it's TTL is decremented by 1. At the second router the TTL reaches 0. This causes the second router to return an ICMP Time To Live exceeded message which reveals ip address of that router. This process continues until the packet reaches its destination.

An ARP table is a cache of MAC address to IP address associations. The arp table can be viewed with the command "arp –a"

DNS is a software program that runs on a server and translates domain names into IP addresses. When your computer needs to know the IP address for yourdomain.com it asks a DNS server (usually provided by your ISP.)

There are ten's of thousands of DNS servers, however they all trace back to a few "authoritative" DNS servers.

DHCP (Dynamic Host Configuration Protocol) has 3 allocations methods:
Automatic, Dynamic and Manual

DHCP is defined in RFC 2131.

The DHCP client broadcasts a DHCPDISCOVER packet.
A DHCP server returns a DHCPOFFER packet.
The client may receive multiple DHCPOFFER packets.
The client chooses a DHCP server based on the DHCPOFFER packet.
The client sends a DHCPREQUEST packet to the server.
The server responds with a DHCPACK message and the lease is finalized.

Know the following about IPv4 addresses:

IPv4 address structure is in (dotted decimal) xxx.xxx.xxx.xxx

CIDR notation represents a subnet mask as a decimal number representing the series of contiguous 1s (255.255.255.0 would be represented as /24).

IPv4 class A, B and C address ranges

Class A 1.0.0.0 - 126.255.255.255
Class B 128.0.0.0 - 191.255.255.255
Class C 192.0.0.0 - 223.255.255.255

IPv4 class A, B and C address structure (Network & Host portion)

Class A N.H.H.H
Class B N.N.H.H
Class C N.N.N.H

Private address for class A, B and C

Class A 10.0.0.0 - 10.255.255.255
Class B 172.16.0.0 - 172.31.255.255
Class C 192.168.0.0 - 192.168.255.255

Directed broadcast – Broadcasts to the entire network (ex. 172.16.255.255 would broadcast to all devices on the network and is capable of being routed)

Local broadcast – (255.255.255.255) would broadcast to all devices on the network and is NOT capable of being routed)

Local loopback – (127.0.0.1)

Autoconfiguration IP address – When no address is found on startup an address in the range of 169.254.0.0 /16 is assigned to the interface.

Be able calculate subnet information (number of networks, number of hosts, networks address, 1st usable, last usable and broadcast) – use my "Eight steps to subnettng success"

Be able to **design subnet solutions** (see my "Subnet Design" video)

Be able to design **a simple VLSM scheme** (see my video, VLSM for help).

Know that in order for two different networks (or sub-networks) to communicate, they must talk through a router. The router that a host uses to communicate with the rest of the network is called the default router or **default gateway**.

Be able to:

Convert Binary to Decimal – add the base 2 values of every column with a value of 1

Convert Decimal to Binary - find a base 2 column larger than the decimal number you wish to convert to binary, try to subtract the next smaller column from your decimal number (if this is passable, put a 1 in this column), repeat this process until you reach 0.

Covert between Hexadecimal, Decimal and Binary – 1st convert the Hex digit to decimal the convert to binary.

See my video (**binary basics**) for help with this.

Know the following Layer 4 facts:

Transport layer is responsible for: Session multiplexing, segmentation, flow control, and reliability (error correction)

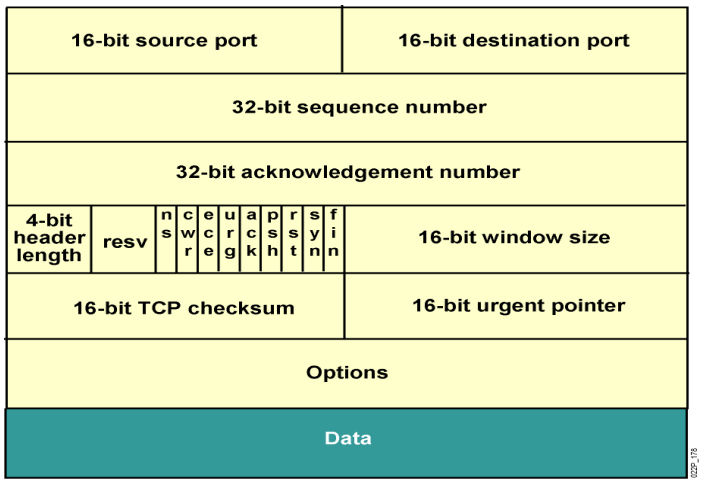
UDP characteristics: Connectionless, best effort with no guarantees
UDP applications: real time and polling (voice/video and SNMP)

TCP characteristics: Connections, full duplex, error checking, sequencing and acknowledgements, flow control packet retransmission
TCP applications - used when traffic must be accurately transferred.

Common TCP ports: FTP (20&21), SSH (22), Telnet (23), SMTP (25) DNS (53) and WWW (80)

Common UDP port numbers: DNS (53), TFTP 69, and SNMP 161

The structure of **UDP and TCP headers**



TCP fields:

Source & Destination ports

Sequence number

Acknowledgement number

Syn & Ack bits

Window size

The process of establishing a TCP connection

> **The source PC sends** a TCP packet to destination PC with the SYN bit set to 1 – This is interrupted as "can we talk?".
>
> The destination PC receives the **SYN** packet and responds with a packet that has both the SYN and ACK bits set to 1 – This is interrupted as "Yes, we can talk".
>
> **The source PC the sends** a TCP packet to destination PC with only the ACK bit set to 1 – This is interrupted as "Consider us talking".**TCP flow control** (sliding window sizes) – the receiver controls he amount of data it receives by changing the window size which controls the amount of unacknowledged data that can be sent to the receiver.

TCP sequencing and acknowledgment: The receiver sends an acknowledgment number which is equal to the senders sequence number + the number of bytes of data + 1

TCP/UDP Ports numbers from 0 to 1023 are **well known ports**

TCP/UDP **registered ports** are from 1024 through 49151.

Understand the characteristics of the three types of routing protocols:

Distance vector algorithms are based on the work done of R. E. Bellman and L. R. Ford and are referred to as *Bellman-Ford* algorithm.

With distance vector protocols, routers trade routing protocols periodically (in the case of RIP, every 30 seconds). Routes are advertised as vectors (distance, direction), where distance is defined in terms of a metric and direction is defined in terms of the next-hop router. - RIP

Link State protocols flood routing information to all nodes in the network. Each router, however, sends only the information that describes the state of its own links. Then, each router builds a database of the entire network in its routing tables based on the link state advertisements it has received using the SPF (shortest path first) algorithm. – OSPF

Hybrid/Advanced Distance vector - EIGRP

Understand that an **Autonomous System (AS)** is a group of networks administered by one organization – routing protocols used inside of an AS are called **Interior Gateway Protocol** – RIP, OSPF, IGRP, EIGRP. IS-IS – the routing protocol that routes between AS's is called an **Exterior Gateway Protocol** – BGP4

Be well versed in CDP:

CDP is a Cisco proprietary Layer 2 protocol that discovers directly connected devices

LLDP is a standardized alternative to CPP

#show cdp neighbors – gives a brief description of device ID, platform, local and connected interfaces and capabilities

#show cdp neighbors detail – displays a detailed description of directly connected devices including neighbor IP address and IOS version.

Know that **assigning an IP address to an interface** is executed at the configure interface prompt by entering **ip address** followed by the ip address and the subnet mask

(config-if)#ip address 172.16.1.5 255.255.255.0

Understand that the **show ip interface brief** command provides a detailed description of an interface**.** The first line describes the physical layer condition (up, down, administratively down) and the status of Layer 2 (up, down). Up and down are self explanatory, administratively down means the administrator has turned the interface off.

Know that bouncing an interface will clear some problems –

(config-if)#shutdown
(config-if)#no shutdown

#telnet 10.0.0.1 remotely access the device at the ip address 10.1.1.1

#show sessions – shows my telnet sessions

#show users -shows users telneting into my router

Suspend a telnet session <ctrl-shift-6>x

Resume a telnet session – resume # (# is the session number)

 # disconnect closes the current telnet session opened by you

 # clear line x close a telnet session opened by a remote user (x is the number displayed by the "show users" command)

MASTER THE PACKET DELIVERY PROCESS EXPLAINED IN YOUR COURSE MATERIAL!!!

Know that **static routes** are configured by administrators, can precisely control packet, use few router resources and routing can not be quickly changed

Know that **dynamic routes** are learned by routing protocols and are automatically changed, can NOT precisely control packet and use significant router resources

A stub network has only one-way in and one-way out

Static route: **(config)# ip route (dest address) (mask) (next hop|local port)**

Default route: **(config)# ip route 0.0.0.0 0.0.0.0 (next hop|local port)*Know the following information about Access Control Lists (ACL)***

Access Control Lists filter traffic going through a router

Wild card masks can be calculated by subtracting a subnet mask from 255.255.255.255

Standard Access Control Lists filter on **source IP addresses** only and use access list numbers from **1-99** and **1300-1999**

Extended Access Control Lists filter on source IP, destination IP and all protocols (ICNP, UDP, TCP) and their ports and are identified by ACL numbers **101-199** and **2000-2699**

Know the rule: **one ACL per interface, per direction, per protocol**

ACLs process from the top down and have an implicit "deny all" at the end

"host x.x.x.x" is a shortcuts for "x.x.x.x 0.0.0.0"

"any" is a shortcut for "0.0.0.0 255.255.255.255"

Place standard ACLs as close to the destination as possible – extended ACLs as close to the source as possible

Know the basic structure of an access-list that blocks a network:

(config)# access-list 10 deny192.168.3.0 0.0.0.255
(config)# access-list 10 permit any

Know the structure of an extended access-list that blocks only one network from www access

(config)# access-list 101 deny tcp192.168.3.0 0.0.0.255 any eq 80
(config)# access-list 101 permit ip any any

To apply an access list to a physical interface:

(config)#int e 0
(config-if) ip access-group 101 out

To apply and access to a vty interface:

(config)#line vty 0 4
(config-if) access-class 15 in

#show ip interfaces will display the inbound and outbound access list applied to each interface

#show access-list shows the ACLs in memory and their content

(config)#no access-list xxx removes the ACL from the router but NOT from an interface until the next reload

(config-if)#no ip access-group # in|out removes the ACL from an interface

(config-if)#no access-class # in|out removes the ACL from a vty interface

Know the following about NAT (Network Address Translation)

NAT benefits simplifies management, conserves address space and improves security

3 Types of NAT

Static NAT
Dynamic NAT
PAT (Port Address Translation)

Nat terms:

- **Inside address -** points to a host inside my network.
- **Local address** - The address we are translating from, hidden fro the outside network and usually a private address.
- **Outside address** – points to a host outside of my network.
- **Global address** - A legitimate (ICANN/IANA issued) IP address that represents one or more inside IP addresses to the outside world.

Static NAT translates ip addresses on a one for one basis.

Dynamic NAT translates a group of ip addresses (often one or more subnets) to a (usually) smaller group of ip addresses a first come first serve basis.

Overloading is also known as Port Address Translation and maps multiple inside local address to a single inside global address. The L4 port addresses are used to keep track of the individual translation.

3 Steps to configure static NAT

1. Define an interface as NAT inside
2. Define an interface as NAT outside
3. Establish static translation

Example:

(config)#interface e 0
(config-if)# ip address 10.10.10.254 255.255.255.0
(config-if)# ip nat inside
(config-if)# end
(config)# interface s 0
(config-if)#ip address 172.16.130.2 255.255.255.0
(config-if)#ip nat outside
(config-if)# end
(config)# ip nat inside source static 10.10.10.1 172.16.131.1

5 Steps to configure dynamic NAT

1. Define an interface as NAT inside
2. Define an interface as NAT outside
3. Define a pool of global addresses to be used as needed
4. Use a standard ACL to define the local address to be translated
5. Establish dynamic translation specifying the ACL to be used

Example of dynamic nat:

(config)#interface e 0
(config-if)# ip address 10.10.10.1 255.255.255.0
(config-if)# ip nat inside
(config-if)# end
(config)# interface s 0
(config-if)#ip address 172.16.130.2 255.255.255.0
(config-if)#ip nat outside
(config-if)# end
(config)#ip nat pool test 172.16.130.97 172.16.130.110 netmask 255.255.255.240
(config)#access-list 10 permit 10.10.10.0 0.0.0.255
(config)#ip nat inside source list 10 pool test

4 Steps to configure NAT overloading

1. Define interfaces as NAT inside
2. Define an interface and ip address as NAT outside
3. Define a standard ACL to define the local address to be translated
4. Establish dynamic translation specifying the ACL and overload mode

Example of NAT Overloading:

(config)#interface e 0
(config-if)# ip address 10.10.10.1 255.255.255.0
(config-if)# ip nat inside
(config)#interface e 1
(config-if)# ip address 10.10.11.1 255.255.255.0
(config-if)# ip nat inside
(config-if)# end
(config)# interface s 0
(config-if)#ip address 172.16.130.2 255.255.255.0
(config-if)#ip nat outside
(config-if)# end
(config)#access-list 10 permit 10.10.10.0 0.0.0.255
(config)#access-list 10 permit 10.10.11.0 0.0.0.255
(config)#ip nat inside source list 10 interface serial 0 overload
(config)#ip route 0.0.0.0 0.0.0.0 serial 0

#clear ip nat translation * - clears all dynamic translations

 # clear ip nat translation [inside global-ip local-ip] [outside local-ip global-ip] clears a specific ip nat translation

#sh ip nat translations - displays the number of active translations

#sh ip nat statistics - displays the number of active translations

Know these miscellaneous router commands:

Set the size of the history buffer: (config)#line console 0
(config-line)# history size *lines*

Set device name: (config)# hostname *name*

Redisplay interrupted input: (config)# line console 0
(config-line)#logging synchronous

To **assign an IP address to an interface** enter the interface configuration mode and enter the command **ip address** followed by the ip address and the subnet mask

(config-if)#ip address 172.16.1.5 255.255.255.0

To assign an interface as a **DHCP client** enter the interface configuration mode and enter the command **ip address** followed by the key word ***DHCP***

(config-if)#ip address dhcp

Modify time out on a line:

(config)# line console 0
(config-line)#exec-timeout 20 30 [20 min 30 sec

Redisplay interrupted input:

(config)# line console 0
(config-line)#logging synchronous

Configure Security on a router:

Set Message Of The Day:

(config)# banner motd # *message* #

Set Login Banner:

(config)# banner login # *message*#

Set Console password:

(config)#line console 0
(config-line)#login
(config-line)#password xxxxx

Set Virtual Terminal password:

(config)#line vty 0 4
(config-line)#login
(config-line)#password xxxxx

Set SSH:

(config)#username bob password secret
(config)#ip domain-name test.com
(config)#crypto key generate rsa
(config)#ip ssh verson 2
(config)#line vty 0 4
(config-line)#login local
(config-line)#transport input ssh

The enable password is an unencrypted password protecting the privileged mode. It is used for compatibility with older "legacy" systems only.
Enable password (config)#enable xxxx

The service password encryption command provides a very weak encryption for the enable password. It is used for compatibility with older "legacy" systems only.
Service password encryption (config)#service password-encryption

The Secret password is a strongly encrypted password and should be used whenever the IOS release supports it.
Enable secret password (config)#enable secret xxxx

External Authentication can be configured with a **RADIUS** or **TACACS** server.

NTP (Network Time Protocol) synchronizes the time on all routers and switches in your network. This is useful for troubleshooting and authentication with digital certificates.

A router or switch can act as a network NTP server, or the network can use an Internet clock or atomic clock (GPS).

Set router as NTP client (config)#ntp server 10.1.1.1

Understand the configuration of a DHCP sever:

```
(config)#ip dhcp pool test
  (dhcp-config)#network 192.168.1.0 255.255.255.0
  (dhcp-config)#default-router 192.168.1.1
  (dhcp-config)#domain-name example.com
  (dhcp-config)#dns-server 172.16.1.99 172.16.3.55
  (dhcp-config)#lease 1
(config)ip dhcp excluded-address 192.168.1.0 192.168.1.99
```

View details about the DHCP pool: **show ip dhcp pool**

View mac address to IP address binding: **show ip dhcp binding**

View multiple devices using the same address: **show ip dhcp conflict**

An ***IP helper address*** direct DHCP requests on one subnet to a DHCP server that resides on a different network. Also known as an DHCP Relay Agent .

To configure an ***IP helper address*** on an interface:

```
(config)#interface Ethernet 0
(config-if)#ip helper-address 172.25.1.1
```


Understand and Configure VLANs

VLANs are enforced broadcast domains and are used to make networks easier to manage, enhance network security and enforce QOS.

Switch ports can be in one of two states: Access ports and trunks. Access ports have only one data vlan assigned to it (with the possibility of a voice vlan assigned also), trunks (in their default state) have all the vlans in the network.

A device attached to an access port is a member of the vlan assigned to that port and can only communicate with other devices on that same vlan.

By default all ports are in access mode and members of vlan 1

To put an interface in trunk or access mode:

(config-if)# switch port mode (truck| access)

To create a vlan

(config)#vlan 2
(config-vlan)#name xxxx (names are optional)

To delete a vlan

(config)#no vlan 2

To assign a vlan to a port:

(config)# fa 0/2
(config-if)#switchport mode access
(config-if)#switchport access vlan 2

To remove a vlan from a port:

(config)# fa 0/2
(config-if)#no switchport access vlan 2

802.1q is the IEEE standard based tagging used for a trunk.

The **Native VLAN** allows non-vlan protocols to participate in LAN – it is untagged and by default VLAN 1

To change the native vlan:

(config-if)# switchport mode trunk
(config-if)# switchport trunk native vlan 35

Dynamic Trunk Protocol (DTP) is a Cisco proprietary protocol designed to automatically negotiate trunking between two Cisco switches.

Know the combinations of DTP states and the port states they will result in.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	**Access**	**Trunk**	**Trunk**	**Access**
Dynamic Desirable	**Trunk**	**Trunk**	**Trunk**	**Access**
Trunk	**Trunk**	**Trunk**	**Trunk**	**Not recommended**
Access	**Access**	**Access**	**Not recommended**	**Access**

Use the **show interface fa 0/1 trunk** to verify that the port is in trunk mode and that that all necessary vlans can travel across it.

To limit the vlans that can move across a trunk

(config-if)#switchport trunk allowed vlan 5-60

To add a vlan to a trunk with an existing vlan allowed statement applied to it:

(config-if)#switchport trunk allowed vlan add 77

To remove a vlan from a trunk with an existing vlan allowed statement applied to it:

(config-if)#switchport trunk allowed vlan remove 10

Routing between two valns can be accomplished in 3 ways:

Each vlan is connected on a separate router port
Vlans routed through a multilayer switch
Router attached to switch via a trunk (router on a stick)

Configure "router on a stick" for 802.1q on the router interface:

(config)#interface fa 0/0
(config-if)#ip address 172.16.33.2 255.255.255.0
(config-if)#interface f0/0.2
(config-subif)#encapsulation dot1q 2
(config-subif)#ip address 192.168.7.2 255.255.255.0

Know that **WAN**s communicate between LANs over large geographic areas.

Understand the three technologies used for WANs are: dedicated, switched and Internet.

Know the following facts about IPv6:

IPv6 has a much larger address space, a simpler header than IPv4. It also has native support for IPSec.

IP v6 has 128 address fields and is expressed as a series of 16 bit fields in 4 character hexadecimal format separated by colons: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

Leading zeros between two colons are optional.

Once (and ONLY once) in an address, a string of zeros can be **compressed to ::**

IP v6 address types:

Unicast: one to one
Multicast: one to many
Anycast: one to nearest

Global IPv6 Unicast addresses assigned by IANA beginning with 2000::/3

Private Addresses begin with FE80::/10

Link local – NOT routable – valid on a local link only! FE80::/10

Loopback Address – 0:0:0:0:0:0:0:1 = ::1

Currently, the first 23 bits identifies the global registry that this IP originates from, the net 9 bits identifies the ISP that this IP originates from, the next 16 bits identifies the customer site that this IP is associated with the next 16 bits identifying subnet within the organization that IP is associated with.

EUI-64 is a standard that assigns the last 64 bits of an address by modifying the interface's MAC address. The 48 bits of the MAC address is split in half. Between the two halves the hexadecimal number **FFFE** is inserted. The result is a 64 bit host portion that is unique on this LAN.

There are two types of EUI-64 addresses: **Universally Unique** and **Locally Unique**. Universally unique addresses are unique throughout the Internet. Locally unique addresses are unique only on a LAN.

Universally Unique addresses are identified by forcing **bit 7** of the **first octet** of the **OUI** to a **value of 1. Locally Unique** addresses are identified by forcing **bit 7** of the **first octet** of the **OUI** to a **value of 0.**

Every interface has **AT LEAST 2 addresses** – 1 loopback and 1 link local

Global IP addresses can be assigned in 4 ways

Static Manual
Static EUI-64
Dynamic Stateless Autoconfiguration
Dynamic DHCPv6

Routers supporting IPv4 and IPv6 must be **Dual Stacked**. **Dual Stacking** means that the router supports both IPv4 and IPv6. Dual Stacking is necessary on routers tunneling IPv6 across IPv4 and to support NAT proxying (IPv4 to IPv6 translation).

To turn on IPv6 on a router: **(config)#ipv6 unicast-routing**

Apply an IP v6 address to an interface manually (X is your host address)

(config)#ipv6 unicast-routing
(config)#int fa 0/0
(config-if)#ipv6 address 2001:dd45:c77:2::X/64 eui-64

Apply an IP v6 address to an interface using EUI-64

(config-if)#ipv6 address 2001:dd45:c77:2::/64 eui-64

Traceroute, ping, telnet and ssh commands in IPv6 have the same syntax as these commands have in IPv4.

ICMPv6 supports echo request, echo reply, router solicitation, router advertisement, neighbor solicitation and neighbor advertisement.

ICMPv6 router advertisement is type 134. Destination address is FF02::1

ICMPv6 router solicitation is type 133. Destination address is FF02::2

Neighbor discovery is accomplished with ICMPv6 and is **similar to ARP**.

In Stateless Autoconfiguration the local router sends out ICMPv6 router advertisements (type 134) on the LAN periodically using the all nodes multicast address. A host sends out a ICMPv6 router solicitation (type 133) at bootup. When the host receives a response (or a router advertisement) it uses the router address to identify the host's default gateway. The host also uses the network portion of the router address as it's own network address and uses the EUI-64 process to self assign a unique host address.

Stateless Autoconfiguration - **(config-if)#ipv6 address autoconfig**

Like IPv4, IPv6 has Interior Gateway Protocols for routing inside an Autonomous System and Exterior Gateway Protocols for routing between Autonomous Systems.

IPv6 Interior Gateway Protocols include: static, RIPng, EIGRP for IPv6 and OSPFv3.

The Exterior Gateway Protocol for IPv6 is MP-BGP4

IPv6 static routes are configured similarly to IPv4 static routes but includes both the next hop IPv6 anddress AND the outgoing interface.

(config)#ipv6 route ***destination_address outgoing_interface next_hop***

Understand how Spanning Tree Protocol (STP) provides loop free redundant topology.

802.1d is the IEEE's definition of classic spanning tree protocol. Convergence takes from 30 to 50 seconds. **802.1d** is sometimes called **Common Spanning Tree (CST)** and does not allow load balancing between vlans.

PVST+ is Cisco's proprietary implementation of 802.1d on a per-vlan basis. This provides basic load distribution, but is more taxing to the CPU than CST.

802.1w is the IEEE's definition of the rapid spanning tree protocol. **Rapid Spanning Tree Protocol (802.1w)** quickly moves edge ports and point-to-point links to the port forwarding state. Convergence takes from 2 to 4 seconds and more CPU resources than CST but less than PVST+.

Rapid PVST+ is Cisco's proprietary implementation of 802.1d on a per-vlan basis and uses the most CPU resources of any spanning tree method.

In classic spanning tree the root switch is the only switch allowed to produces a **BPDU (Bridge Protocol Data Unit) packet**. By default these packets are sent out every port of the root switch every two seconds. Other switches forward BPDU packets out of all non-blocked ports.

The BPDU contains a number of fields including: the bridge ID, the root ID, and the cost.

Each switch has a **Bridge ID** that is made up of the switch Priority + the lowest MAC address on the switch.

The **root bridge** is the switch with the lowest Bridge ID.

There is **one root port per bridge**, the root port has the lowest path cost from the bridge to the root bridge.

Each **LAN segment has one Designated Port** which provides the only path on the LAN segment to the Root Bridge. The **Designated Port** is the port on the LAN segment with the **lowest cost to the root bridge.** By definition, all ports on a root switch are **designated.**

All ports that are **not designated and not root** are blocked

Link Speed	Cost
10 Gbps	2
1 Gbp	4
100 Mbps	19
10 Mbps	100

The IEEE uses these **costs for spanning tree links**

Know the four states a spanning tree port transitions through

Blocking (receives BPDU's - does not process them, asks "am I the root?")
Listening (sends, receives and PROCESSES BPDUs only – no Ethernet traffic)
Learning (creates a MAC database – does not forward)
Forwarding – acts like a full switch

Spanning tree port rolls:

Root port - The port on a switch which provides the lowest cost path back to the root. There is only one root port per switch.
Designated port – The one port on a LAN segment which provides the lowest cost path back to the root switch.
Non-designated port - Does not forward data, it is blocked.

PVST+ and Rapid PVST+

In common spanning tree (CST) there will always be at least one link that has no traffic. This is not an efficient use of bandwidth. Cisco created Per Vlan Spanning Tree (PVST) in order to distribute traffic across all the links in your life. In order to accomplish this distribution of traffic, PVST allows you to have a separate root switch for each VLAN in your network. It accomplishes this by taking the bridge ID (which is a 16 bit binary word) and using the most significant bits as the switch priority number and the remaining bits to identify the VLAN that this BPDU is associated with.

An **Extended Bridge ID** divides the 2 Byte Bridge priority field into two parts: a 4 bit bridge priority number and a 12 bit Extended ID field (which indicates the VLAN ID for use PVST+.)

Cisco switches do not support 802.1d or 802.1w. Instead they support PVST+ which is 802.1d implemented on a per vlan basis and rapid PVST+ which is 802.1w implemented on a per vlan basis.

Set rapid-pvst+ for the switch

(config)#spanning-tree mode rapid-pvst

Port Fast – is used to causes a port to enter the forwarding state almost immediately and is used ONLY on ports which DO NOT participate in spanning tree i.e ports connected to hosts, servers and routers.

Configure portfast on a port

(config)#interface fa 0/0
(config-if)# spanning-tree portfast

BPDU guard shuts ports down when a BPDU is detected. It is used to protect ports configured as "portfast" from connecting to a switch and causing a loop.

(config)#spanning-tree portfast bpduguard to apply bpduguard globaly
(config-if)#spanning-tree bpduguard enable to apply bpduguard on a port

Configure a switch as root for VLAN 1

(config)#spanning-tree vlan 1 root primary

Configure a switch as the back up root for VLAN 1

(config)#spanning-tree vlan 1 root secondary

Configure the priority manually a switch for VLAN 1

(config)#spanning-tree vlan 1 priority 4096

Spanning tree on a vlan can be verified with **show spanning-tree vlanX**

From the show spanning-tree output be able to determine the type of spanning tree protocol, root bridge ID, the priority number of the bridge, the Bridge ID of this switch.

```
#sh spanning-tree vlan 10
        VLAN00010
          Spanning tree enabled protocol rstp[1]
          Root ID    Priority    4106
                Address     0008.e3ce.3cc0
                This bridge is the root[2]
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

          Bridge ID  Priority    4106[3]  (priority 4096[4] sys-id-ext 10)
                Address     0008.e3ce.3cc0
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                Aging Time 300

        Interface        Role Sts Cost      Prio.Nbr Type
        ---------------- ---- --- --------- -------- --------------------------------
        Fa0/1            Desg FWD 19        128.1    P2p Peer(STP)[5]
        Fa0/7            Desg FWD 19        128.7    P2p
        Fa0/9            Desg FWD 100       128.9    Shr
        Fa0/11           Desg FWD 19        128.11   P2p Peer(STP)
        Fa0/12           Desg FWD 19        128.12   P2p Peer(STP)
        Fa0/15           Desg FWD 100       128.15   Shr
        Fa0/23           Desg FWD 19        128.23   P2p
```

1) **This bridge is running RSTP (802.1w) if it were 802.1d it would display ieee.**
2) **This is the root bridge**
3) **The priority of this bridge**
4) **The base priority which is the priority minus the vlan ID**
5) **This port is attached to an 802.1d switch**

Understand EtherChannel

Logical aggregation of between 2 and 8 channels (Base 2 multiples).

EtherChannel Rules

Interfaces do not need to be contiguous.
Port costs can be different.
All interfaces must be in the same speed and duplex mode
One of the interfaces can not be an analyzer destination port.
All interfaces must have the same vlans assigned or be configured as trunks
IP address must be assigned to the logical port – not a physical interface
Port channel changes affect the EtherChannel.
Physical interface changes affect that interface only.

PAgP (Port Aggregation Protocol) is a Cisco proprietary EtherChannel trunking protocol.

Understand the **interaction of PAgP options**: On, Desireable and Auto.

PAgP Options

> **(config-if-range)#channel-protocol pagp** - Enables the Cisco proprietary protocol
> **(config-if-range)#channel-group 1 mode desirable** - Enable PAgP unconditionally
> **(config-if-range)#channel-group 1 mode auto** - Enable PAgP if a PAgP device is detected

LACP (Link Aggregation Control Protocol) is an IEEE standard EtherChannel protocol.

Understand the **interaction of LACP options**: On, Active and Passive.

Configure **LACP Options**

> **(config-if-range)#channel-group 1 mode on** - Enable Etherchannel - no PAgP or LACP
> **(config-if-range)#channel-protocol lacp** – Enables the IEEE standard protocol
> **(config-if-range)#channel-group 1 mode active** - Enable LACP unconditionally
> **(config-if-range)#channel-group 1 mode passive** - Enable if a LACP device is detected

Configure EtherChannel

> (config)#interface range *interface slot/port - port*
> (config-if-range)#channel-protocol {pagp | lacp}
> (config-if-range)#channel-group *number* mode {auto | desirable | on}

#show interface port-channel 1 to display the state of the Etherchannel

#show etherchannel summary to display a brief summary of each etherchannel, the trunking protocol used, and the ports bundled in etherchannel.

#show etherchannel port-channel

Understand First Hop Redundancy Protocols

First Hop Redundancy Protocols (FHRP) are designed to allow for transparent fail-over at the first-hop IP router (i.e. default gateway).

HSRP is a Cisco proprietary method of combining multiple routers into one virtual router. An HSRP virtual router presents a virtual IP and virtual MAC to hosts.

One router in an **HSRP group is active** (i.e. processing all frames and packets sent to the virtual MAC address and the virtual IP address.) The **HSRP active router:**

Responds to all ARP requests directed to the Virtual IP
Forwards packets addressed to the virtual router
Sends Hello (keep alive) messages
Knows the IP address of the virtual router

One router in the **group acts as the Standby router** and is the primary backup router. The **HSRP standby router:**

Listens for Hello (keep alive) messages.
In the absence of Hello (keep alive) messages, takes on roll of Active Router.

All other routers in an HSRP group are members of the **standby group.**

Each router in an HSRP group has a priority number. The router with the highest priority becomes the active router.

HSRP interface tracking enables the priority of an HRSP router to be changed based on state of a WAN based interface.

Traffic can be distributed between routers in an HSRP group by making one router the active router for hosts in vlan 10 and making other other router the active router for hosts in vlan 20.

VRRP (Virtual Router Redundancy Protocol) is a non-proprietary protocol that performs functions like HSRP.

GLBP is a Cisco proprietary protocol similar to HSRP. However, with GLBP traffic is distributed between routers automatically. A GLBP group provides a single IP and multiple virtual MACs.

Know WAN Technologies

WANs have large geographic areas, owned by service providers, slower than LANs,
LANs have small geographic areas, owned by end users, faster than WANs,
WAN use OSI Layers 1 & 2

There are 3 types of WAN connections: Dedicated (leased lines), Switched (Frame Relay, ATM, MPLS) and datagram (Internet)

DTE: **D**ata **T**erminal **E**quipment (source or destination of network signals)

DCE: **D**ata **C**ircuit-terminating **E**quipment (convert signals for transmission)

DB 60 is a cisco proprietary connecter (Old)

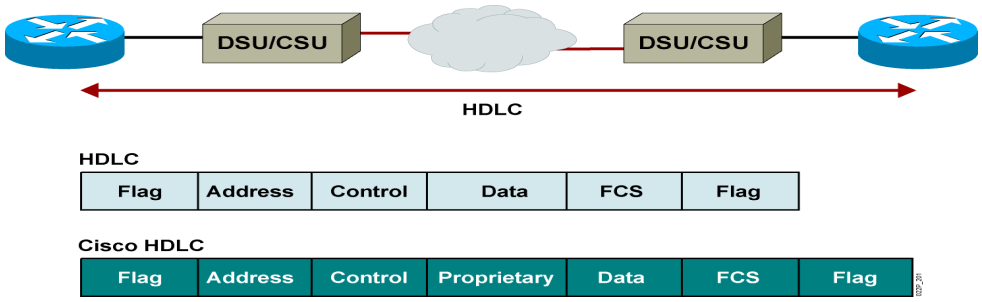
Smart Serial is a cisco proprietary connecter (New)

EIA/TIA-232 is a standards based connecter with a maximum speed of 64kb/s.

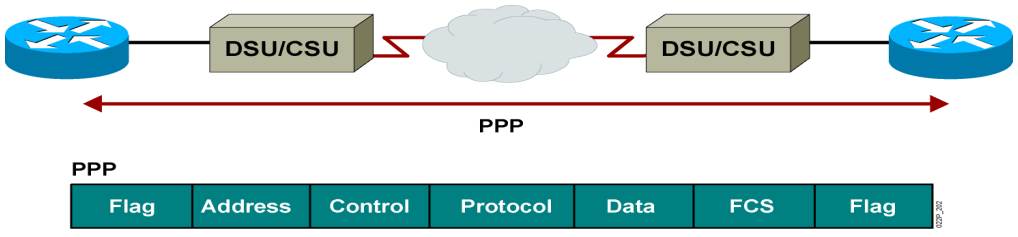
V.35 is a standards based connecter with a maximum speed of 2.048mb/s.

HDLC is used in Point To Point environments, is open source, simple, but only supports a single layer 3 protocol (i.e IPv4 OR IPv6 – not both)

Cisco HDLC is used in Point To Point environments, is proprietary, simple, and supports a multiple layer 3 protocol



PPP is used in Point To Point environments, is open source, supports authentication, compression, and multiple layer 3 protocols. Used to connect to non-Cisco equipment.



The bandwidth command sets the bandwidth metric of the interface.

The clockrate command sets clock speed on a DCE interface

Example serial WAN configuration:

(config)#interface S 0/0
(config-if)# ip address 10.10.10.254 255.255.255.0
(config-if)# bandwidth 64
(config-if)# clockrate 64000

The Show controllers command displays layer 1 information bout the interface

Characteristics of **Circuit switching** – Fixed path & Fixed bandwidth

Characteristics of **packet switching** – Variable sized addressed packets, no dedicated bandwidth, no fixed path.

Characteristics of **Virtual Circuits** – Fixed path & fixed bandwidth

(config-if)# encapsulation hdlc|ppp configures hdlc or ppp on a serial port

In PPP, NCP supports multiple network layer protocols, LCP supports authentication, compression, error detection and inverse multiplexing (Multi link PPP)

(config)#username xxxxx password yyyyy set user name and password of remote router (password of local and remote routers must match)

(config-if)# ppp authentication {chap | chap ppp | ppp chap | ppp} sets the authentication

Use "show interface" command and "debug" command to verify chap

Understand and configure Frame Relay

Frame Relay characteristics - Virtual circuits, variably sized frames, very fast, no error correction

Frame Relay is a layer 2 protocol that operates between the CPE and the edge of the service provider network

Data Link Connection Identifier (DLCI) is a LOCAL address that has NO global significance

CIR - Committed Information Rate, Packets transmitted in excess of this rate will be marked as DE (Discard Eligible)

BECN - Backwards Explicit Congestion Notification, Notifies devices of congestion in the network

FECN - Forward Explicit Congestion Notification, Notifies devices of congestion in the network

DE - Discard Eligible , These frames may be dropped when congestion occurs.

A Non-Broadcast Multiple Access networks **(NBMA)** is used in FR, ATM & X.25. NBMA networks act like the opposite of a hubed Ethernet network. Through a single interface multiple networks can be accessed but frames are not sent to each possible node – only the destination node revives the frame.

A NBMA network is **unsuitable for Distance Vector** protocols because these protocols can not trade routing tables due to the split horizon rule. NBMA networks are suitable for link state protocols.

Point to point frame relay is used to support frame relay on distance vector protocols like EIGRP. This uses more IP addresses than Point to Multipoint.

Point to point subinterfaces example:

#(config)interface Serial 0/1
#(config-if)no ip address
#(config-if)encapsulation frame-relay

#(config-if)interface Serial 0/1.45 point-to-point
#(config-if)ip address 10.17.0.1 255.255.255.0
#(config-if)frame-relay interface-dlci 45

#(config-if)interface Serial 0/1.90 point-to-point
#(config-if)ip address 10.35.0.1 255.255.255.0
#(config-if)frame-relay interface-dlci 90

Point to point frame relay is used to support frame relay on link state protocols like OSPF. This uses fewer IP addresses than Point to Point – but will not support distance vector protocols.

Point to Multipoint example:

#(config)interface Serial 0/1
#(config-if)no ip address
#(config-if)encapsulation frame-relay
#(config-if)interface Serial 0/1.2 multipoint
#(config-if)ip address 10.0.0.1 255.255.255.0
#(config-if)frame-relay map ip 10.0.0.2 50 broadcast
#(config-if)frame-relay map ip 10.0.0.3 60 broadcast
#(config-if)frame-relay map ip 10.0.0.4 70 broadcast

Inverse ARP maps an local DLCI to an remote IP address

Link Management Interface (LMI) – sends info about active DLCIs and keep alive signals

Frame Relay uses **3 LMI standards Cisco, ANSI Annex D, ITU-T Annex A**

Cisco LMI is used by default

Example of a simple FR interface:

(config)# interface Serial1
(config-if)# encapsulation frame-relay
(config-if)# frame-relay lmi-type cisco

#**show frame-relay map** shows IP address to DLCI association

#**show clear frame-relay-inarp** clears IP address to DLCI association

#**show frame-relay lmi** shows LMI type, Status enquiries sent and received

#show frame-relay pvc shows data packets, FECN, BECN, DE and dropped packets

#**debug frame-relay lmi** shows LMI transactions

Know these troubleshooting principles

Troubleshoot using the OSI 7 layer model

Use show interface and show cdp neighbors for layer 1 & 2
Use ping and traceroute to verify Layer 3 functionality
Use telnet to test layer 4 and above (telnet www.test.com 80)

Troubleshoot Serial and Ethernet Connections

Use show controllers to identify which side of a serial cable is DTE or DCE
Physically inspect the cables
Apply clocking to the DCE side of serial cables
Use show interface to check the ip address and subnet mask on an interface
Bounce the interface
Check for matching duplex and speed settings on Ethernet

Troubleshoot subnet problems

Ensure that no host address is assigned to a network or broadcast address
Check for overlapping VLSM subnets

Troubleshoot OSPF networks

Use show running configuration to identify OSPF configuration
Ignore the OSPF PID - it has no effect on communications between routers
Ensure that attached routers have the same: area number, hello and dead timers, stub area flag and passwords.
Use debug ip ospf packets to verify that ospf hello packets are being exchanged

REVIEW MODULE 9 LESSON 3 – Troubleshooting EIGRP

Troubleshoot EIGRP networks

Use show running configuration to identify OSPF areas
Ignore the OSPF PID as it has no effect on inter router communication
Ensure that attached routers have the same: autonomous system number, hello and dead timers, K values and passwords.
Use the debug ip eigrp packets command to verify that eigrp hello packets are being exchanged

REVIEW MODULE 8 LESSON 2 – Troubleshooting EIGRP

Troubleshoot Access Control Lists

Check the value of the wildcard masks
Check the order of the ACL tests for proper function
Use the show IP interface command to verify that the ACL has been properly applied to the interface

Troubleshoot NAT/PAT

Check that no ACLs are blocking traffic
Ensure that the ACL is permitting all appropriate networks
Check to see if the inside and outside interfaces have properly applied
Make sure that routing has been enabled

Sometimes when you make a change in the network topology, or fix a topology error, stale entries in the ARP cache or stale entries in the Mac address table (CAM table), can make it appear as though the solution you just applied has had no effect on the network.

In those cases can be useful to **flush the ARP cache** and **empty the Mac address table**.

In Cisco's IOS the command to flush the ARP cache is #**clear arp-cache**

In Windows operating system the command to flush the ARP cache is to click on the Start button – Type in run – when the run widow opens type in **netsh interface ip delete arpcache** then click ok.

On a Cisco switch you would only need to address the ARP cache if you were dealing with a switch management issue. If you are having problems with the management interface than the command to flush the ARP cache is the same as on a router.

To clear the Mac address table on a Cisco Switch **#clear mac address-table dynamic**

In addition to what I have written here, it is extremely important that you review and know well all the information provided for you in **Module 6 - Troubleshooting**. In some ways this may be the most important module in the course

Know what a VPN is and configure a GRE Tunnel

There are two types of VPNs

Site-to-Site VPNs
Remote-Access VPNs

Remote-Access VPNs can be configured using Cisco's easy VPN client (software) and Cisco's easy VPN server (hardware)

IPsec provides: Confidentiality, Data integrity, Authentication and Antireplay protection

VPNs can terminate to routers, firewalls or VPN concentrators.

VPN benefits include cheap, scalable, compatible with any access technology and high security.

Cisco has two SSL VPN solutions: Cisco AnyConnect SSL VPN which uses a client installed on the PC, mobile phone or tablet. The other solution is called Clientless Cisco SSL VPN which uses any web browser to connect to the VPN.

The IPsec framework defines rules for a number of things including which IPsec protocol to use), what encryption protocol will be used and what authentication method both sides will use.

A tunnel puts one protocol into a peer or higher OSI layer protocol i.e. putting one IP packet into another IP packet (layer 3 into layer 3)

Tunneling does not (by itself) provide encryption.

GRE Is a stateless layer4 protocol and is identified by the IP protocol number 47. GRE adds at least 24 bytes of additional overhead.

GRE tunneling example:

#(config)interface tunnel 0
#(config-if)tunnel mode gre ip
#(config-if)ip address 10.0.0.1 255.255.255.0
#(config-if)tunnel source 72.5.8.33
#(config-if)tunnel destination 211.87.63.55

#**show ip int brief -** will show that the tunnel exisits and that it is up

#**show int tunnel** – will show details about the tunnel

#**show ip route** – will show networks reachable through the tunnels

Know the following facts about routing:

Router functions:

Learn network topology (learn changes in the network)
Determine packet forwarding (best path)

Routing tables keep a list destinations and how to reach them

Dynamic routes automatically learn about networks through a routing protocol

Directly connected networks are automatically learned by the router.

Default routes, (aka default router, default gateway, gateway of last resort) is the router a packet should be sent to when the network is NOT directly connect and there is no static or dynamic routing table entry.

Routing metrics – the basis (measurement) on which routers pick the best path

Distance vector algorithms are based on the work done of R. E. Bellman and L. R. Ford and are referred to as *Bellman-Ford* algorithm.

With distance vector protocols, routers trade routing protocols periodically (in the case of RIP, every 30 seconds). Routes are advertised as vectors (distance, direction), where distance is defined in terms of a metric and direction is defined in terms of the next-hop router. Because routers learn about networks from neighbors, who may have learned about the network from their neighbors, and so on, distance vector routing is sometimes referred to as "routing by rumor."

Link State protocols flood routing information to all nodes in the network. Each router, however, sends only the information that describes the state of its own links. Then, each router builds a database of the entire network in its routing tables based on the link state advertisements it has received.

Static routes are configured by administrators and can not be quickly changed

Dynamic routes are learned by routing protocols and are quickly/automatically changed

A stub network has only one way in and out

Static route: **(config)# ip route (dest address) (mask) (next hop|local port)**

Default route: **(config)# ip route 0.0.0.0 0.0.0.0 (next hop|local port)**

An **Autonomous System (AS)** is a group of networks administered by one organization. AS Numbers are assigned by IANA through the regional internet registries (ARIN for North America).

Interior Gateway Protocols – RIP, OSPF, IGRP, EIGRP. IS-IS

Exterior Gateway Protocol – BGP4

3 classes of routing protocols

Distance Vector (RIP, RIPv2)
Link State (OSPF, IS-IS)
Advanced Distance Vector - EIGRP

Administrative Distance is a value of trust – lower the number the more it is trusted

Default Administrative Distances:

RIP - 120
OSPF - 110
IGRP -100
EIGRP - 90
STATIC - 1
DIRECTLY CONNECTED – 0

Master these facts about EIGRP

EIGRP is an advanced distance vector protocol

Exchanges routes – NOT routing tables – with directly connected neighbors. This reduces bandwidth usage.

EIGRP uses the **Diffusing Update Algorithm (DUAL)** to rapidly pick **successor** (best route) & **feasible successor** (backup routes). Both the best routes and back up routes are stored in the topology table – this makes reconvergence very rapid.

The best route to network is called the **Successor route**. The alternate routes (backup routes) to the network are called **Feasible successors**

Only Successor routes are sent to the routing table. Feasible successors are saved in the topology table.

Advertises routes using the multicast address: 224.0.0.10

3 tables maintained

EIGRP Neighbor Table – lists directly connected routers
EIGRP Topology table – list all EIGRP routes
Routing Table – list best routes

EIGRP: has 255 hop limit (100 default) uses a composite metric (BW **[k1]** **default**, loading **[k2]** Delay **[k3]** ***default***, reliability **[k4]**, the fifth metric, mtu **[k5]** was never implemented)

EIGRP: Sends hello packets periodically (5 seconds for T1 & up, 60 seconds below T1)

Configure EIGRP:

(config)#router eigrp 100
(config-router)#Network 10.0.0.0

No auto summary command enables support for VLSM

(config)#router eigrp 100
(config-router)# no auto summary
(config-router)#network 10.1.1.0 0.0.0.255

The **passive interface** command usually block out going advertisements only. In EIGRP, the passive interface command block the exchange of hello packets effectively blocking routing information across an interface in both directions.

Configure passive interface:

(config)# router eigrp 100
(config-router)# passive-interface s 0/1

By default, EIGRP load balances across 4 paths that have the same cost. The number of paths can be changed from1 (no load balancing) to 32 with the maximum paths command:

(config)# router eigrp 100
(config-router)# maximum-paths (1 to 32)

EIGRP can load balances across unequal paths using the *variance multiplier* command. Setting this value to 2, if the best route to a network has a metric of 1000 then the router will load balance across any path with a value of 2000 or less.

(config)# router eigrp 100
(config-router)# variance (1 to 128)

#show ip eigrp neighbors displays the neighbor table for EIGRP

#show ip eigrp topology displays networks, Advertised Distance and Feasible Distance to all known networks. **Feasible Distance** is the total cost to the network **- Advertised Distance** is the cost to the destination network as advertised by the neighbor router

#show ip eigrp traffic displays the number of EIGRP packets sent and received

#show ip route eigrp to display the routing table for eigrp only

#show ip protocols commands shows the routing protocols and their associated parameters

#debug ip eigrp shows eigrp neighbor exchanges

EIGRP for IPv6 has only minor differences with EIGRP for IPv4

Three steps to turn on EIGRP for IPv6: 1) turn on IPv6 2) turn on EIGRP IPv6 for the Autonomous System 3) on each interface that you want to advertise on EIGRP IPv6 enter the "ipv6 eigrp" command.

(config)#ipv6 unicast-routing
(config)#ipv6 router eigrp 100
(config)#interface fa 0/0
(config-if)#ipv6 eigrp 100

#show ipv6 eigrp neighbors displays the neighbor table for EIGRP for IPv6.

#show ipv6 eigrp topology displays networks, Advertised Distance and Feasible Distance to all known EIGRP for IPv6 networks.

#show ipv6 route eigrp to display the routing table for EIGRP for IPv6 only.

Understand OSPF networks

OSPF is a link state protocol that converges rapidly, is scalable, and is loop free.

Link state protocols **converge more quickly** and **use less bandwidth** than distance vector protocols, but they use **more memory** and **processor resources** than distance vector protocols. To compensate for this **Link state** protocols break an autonomous system into sub-networks called "Areas".

Uses hierarchical routing **via area 0** to reduce the size of tables and amount of router traffic

If multiple areas exist they must travel though Area 0 (known as the backbone area).

Inside of an OSPF area, routers are known as **"Internal Routers".**

An **Area Boarder Router (ABR)** is a router that connects to the backbone area on one interface and a nonbackbone area on another interface.

An **Autonomous System Boundary Router (ASBR)** connects an OSPF domain (Autonomous System) to a different Autonomous System.

Link State Advertisements (containing Router ID, interface and Bandwidth) are flooded to all routers in an Area. The routers use the **shortest path first (Dijkstra)** algorithm to calculate best path to each network. By default, Cisco routers calculate **Cost** as 100,000,000/BW in bps (T1 is about 66.66)

OSPF load balances across equal paths only, but path cost can be manually configured **(config-if)# ip ospf cost <value>**

The process ID is NOT an AS number and does not need to match other routers an area

All routing protocols use **wild card masks – not subnet masks. A wild card mask** is an INVERTED subnet mask

The **passive-interface** command stops an interface from sending routing updates

The **default-information originate** command announces a default route through OSPF

An OSPF router floods an area with **Link State Advertisements (LSA)** using the IP Multicast Address **224.0.0.5.** This is done once and only repeated under two conditions: 1) if a router experiences a topology change 2) every 30 minutes.

There are 5 types of OSPF message types: Hello, Database Description, Link State Request, Link State Update and Link State Acknowledgment.

OSPF forms a neighbor adjacency with directly connected routers by exchanging hello packets if the Hello/Dead Intervals, Area ID, and Authentication data all match

Hello packets contain:

- Router ID
- Area ID
- DR Address
- BDR Address
- Hello/Dead Interval
- Authentication data

The other types of OSPF message are:

DBD (Database Description) – is a list of all the Link State Advertisements (LSA) that this router knows about.
LSR (Link State Request) – is a request to a neighbor router asking it to send an LSA from the neighbor that this router does not have listed in its database.
Link State Update - is the response to an LSR.
Link State Acknowledgment – is the acknowledgement to an LSU.

Configure a single area OSPF network:

(config)#router ospf 100
(config-router)#network 10.0.0.0 0.0.0.255 area 0
Repeat this command for all the networks attached to this router

Configure an ABR for a multi area OSPF network:

(config)#router ospf 100
(config-router)#network 10.1.1.0 0.0.0.255 area 0
(config-router)#network 10.2.2.0 0.0.0.255 area 1
Repeat this command for all the networks attached to this router

Networks statement can be entered with a **short cut** of the interface IP addressed followed by 0.0.0.0

(config)#router ospf 100
(config-router)#network 10.1.1.1 0.0.0.0 area 0

The process ID is NOT an AS number and does not need to match other routers an area.

A wild card mask is an INVERTED subnet mask.

show ip protocols displays the current configuration of OSPF.

show ip route displays the contents of the routing table.

show ip ospf neighbor shows all the routers that this router has a neighbor adjacency (relationship) with.

#debug ip ospf events shows ospf neighbor exchanges.

show ip ospf interface shows the interfaces that are enabled for OSPF.

In a broadcast networks (as opposed to point to point networks) OSPF elects a **designated router (DR)** and a **backup designated router (BDR)**. To reduce network traffic, the designated router is responsible for generating LSAs for the entire OSPF area.

The OSPF router with the highest Router ID becomes the **designated router**. The highest IP address on the router is chosen as the Router ID, unless there is a loopback address, if so the loopback address becomes the Router ID unless router-id command has been used. The **router-id** command takes precedence over all other methods of ID assignment.

There are **5 BASIC** types of **Link State Advertisements (LSA**)

- ***Type 1*** **- Router LSA** - the router announces its presence and lists the links to other routers or networks in the same area, together with the metrics to them. Type 1 LSAs are flooded across their own area only
- ***Type 2*** **- Network LSA** – generated by the designated router (DR)
- ***Type 3*** **- Summary LSA** - generated by the Area Border Router (ABR) and is generally a summarization of the network in the area.
- ***Type 4*** **– ASBR** - Summary LSA – informs the entire Autonomous System (OSPF Domain) how to reach autonomous system boundary router (ASBR).
- ***Type 5*** **- External LSA** - generated by the ASBR and advertises external networks.

OSPFv2 is used with IPv4. OSPFv3 is used with IPv6.

OSPFv3 is a link state protocol for IPv6

OSPFv3 has only minor differences with IPv6

OSPFv3 is enabled per link – not per network.

The router ID has the same 32 bit format (and same command) as OSPF for IPv4

Adjacencies and next hop information use the IPv6 link-local addresses.

LSA's are sent via the all OSPF router multicast address – FF02::5

Configure OSPFv3

```
(config)#ipv6 unicast-routing
(config)#ipv6 router ospf 1 area 0
(config-rtr)#router-id 0.0.0.1
(config-rtr)#exit

(config)#int fa 0/0
(config-if)#ipv6  address 2001:dd45:c77:2::/64 eui-64
(config-if)#ipv6 ospf 1 area 0
```


show ipv6 ospf displays the current configuration of OSPFv3.

show ipv6 route ospf displays all the ospf v3 routes in the routing table

show ipv6 ospf neighbor shows all ipv6 adjacent neighbors.

show ipv6 ospf interface shows the interfaces that are enabled for OSPF

Understand basic SNMP

SNMP Network Management Systems (NMS) polls SNMP agents (switches, routers, etc.) on the network. SNMP agents are managed nodes and they respond to requests from the NMS. SNMP agents can only send unsolicited information if it the agent has previously defined an event as an SNMP trap.

An SNMP MIB is a standardized database of configuration and alarm states.

SNMP ver 1 uses plaintext authentication and has no bulk retrieval mechanism.

SNMP ver 2c uses plaintext authentication and **has** a bulk retrieval mechanism.

SNMP ver 3 has authentication and privacy and a bulk retrieval mechanism.

(config)# snmp-server community test RO|RW
(config)# snmp-server contact My Name
(config)# snmp-server location My Network

Know simple Syslog use and configuration

Syslog is a protocol that sends notification messages to a destination where they can be retrieved later to aid in security (forensics), and network troubleshooting.

Syslog has 7 levels: 0 (emergency), 1 (Alert), 2 (Critical), 3 (Error), 4 (Warning), 5 (Notice), 6 (Information) 7 (Debugging)

Know the syslog format: %**FACILITY**-**SEVERITY**-**MNEMONIC**: **Message-text**

```
*Jun 12 07:38:34.122 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet 1/4,changed state to up
```

If level 3 is configured then all messages up to level 3 (i.e. levels 7 - 3) will be logged.

Sys Log configuration:

(config)# logging *server_ip_address*
(config)# loging trap *level*

Understand simple NetFlow configuration

NetFlow collects and organizes information about IP traffic. NetFlow reports can inform a network administrator about who is using network resources, how much bandwidth they are using, websites that are being visited, congestion on the network, etc.

A NetFlow enabled device gathers the required information and sends it to a NetFlow collector which analyzes and displays the data.

Cisco defines a flow as a series of packets having a common: source IP address, destination IP address, source port number, destination port number, layer 3 protocol type, ToS field value and input interface.

The three steps to configure NetFlow are: configure what NetFlow data to capture, configure NetFlow where to send the data, and choose the export version.

(config)#interface FastEthernet 0/1
(config-if)#ip flow ingress
(config-if)#ip flow egress
(config-if)#exit
(config)# ip flow-export destination 10.1.1.1 9996
(config)# ip flow-export version 9

Use the "**Show ip int**" command to verify that netflow is configured on an interface

"**Show ip flow export**" displays the export version, the destination IP address and port

"**Show ip cache flow**" displays a summary of netflow statistics.

Master theses basic router facts

The **six steps to bootup** are: POST
Load the bootstrap program
Find the IOS
Load the IOS
Find the configuration file
Load the configuration file

Four types of router memory:
RAM (running IOS and running configuration)
ROM (ROM Monitor & POST),
Flash (compressed IOS)
NVRAM (startup config file and config registry)

Display configuration register with the show version command

Change the configuration register with the (config)# **config-register 0xXXXX** command

Configuration register of **2102** uses IOS in flash and the config file in NVRAM (the normal setting) a register value of **2142** bypasses the config file in NVRAM

The **procedure for password recovery** on the 2600 router:

- Reboot the router with a console session open
- Enter the break during the boot sequence (**Crtl+Break** in hyperterm)
- The prompt should now be: **rommon 1>**
- Type **confreg 0x2142**.
- Type **reset** to reboot the router.
- Copy the startup-config file to the running-config (**copy start run**).
- Change the password (**enable secret**).
- Reset the configuration register (**config-register 0x2102**).
- Copy the running-config file to the startup-config (**copy start run**).
- Reboot the router.

#Show version displays the IOS version, location of the IOS image, the physical interfaces on the router and the value of the configuration register.

#Show flash displays the size of the IOS file, total memory and free memory.

Know the process of Cisco Licensing

Before IOS 15.0 there were eight different IOS software packages that could be purchased depending on the features needed by the enterprise (MPLS, VoIP, VPN, etc).

Beginning with IOS 15.0 there is only one universal software package and it contains all features available on a router.

#show license feature lists all the features you are licensed

The PAK (Product Activation Key) necessary to activate a feature is purchased from Cisco.

To purchase a PAK from Cisco you may need the equipment's **UDI** (Unique Device Identifier) which can be found with the **#show license udi command**

To install a permanent license that you have purchased and stored on flash:

#license install flash0:uck9-2900-SPE150_K9-FHH12250057.xml

Reload the router

Save all licenses to the flash memory:

#license save flash:all_license.lic

To uninstall licenses from a router:

Step 1

(config)#license boot module c3900 technology-package uck9 disable
(config)#exit
#reload

Step 2

#license clear uck9
#configure terminal
(config)#no license boot module c3900 technology uck9 disable
(config)#exit
#reload