

Inter Connecting Network Devices (ICND) 1

This is my personal summary of what I believe are the key points of needed to pass Cisco's CCNA 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!

This material is provided freely for individual, non-commercial use. Any and all commercial use is prohibited. All rights are reserved by TrainingMagic, inc. and the author, Bob Cunningham.

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

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, 2600 or 2800 routers and 2950 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.

Network Component Comparison

Component	Used by a PC	Used by a Switch	Used by a Router
Motherboard	Yes	Yes	Yes
CPU or processor	Yes	Yes	Yes
RAM	Yes	Yes	Yes
ROM	Yes	Yes	Yes
NVRAM	Yes	Yes	Yes
EEPROM or Flash	note 1 No	Yes	Yes
Hard drive	note 2 Yes	No	No
Optical drive	note 3 Yes	Yes	No
Ports	note 4		
Keyboard or mouse port	Yes	No	No
Asynch serial	Yes	Yes	Yes
USB	Yes	No	No
Network	Yes	Yes	Yes
	Modem	See note	See note
Operating system	note 5 Yes	Yes	Optional
Power supply	note 6 Yes	Yes	Yes

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).

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.

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 original **Ethernet frame** and the IEEE **802.3 frame**.

Know the function the Logical Link Control sublayer (802.2) and the Media Access Control sublayer (802.3)

The one LLC provides a standard interface to the network layer. The LLC also provides **Service Access Ports (SAP)** which identify the layer 3 protocol being carried by the LLC frame.

There are several **MAC schemes** that provides a variety of ways to access the physical layer (eg, 802.3 – Ethernet, 802.5 Token Ring, 802.11 Wireless Ethernet)

Ethernet frame is part of the **MAC sublayer**.

You must be able to convert between **Decimal, Binary and Hex**

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 have pin 1 connected to pin 3, and pin 2 is connected to pin 6

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)	-	-

© 2004 Cisco Systems, Inc. All rights reserved.

INTRO v2.0-2-50

Know the physical wiring for the following topologies: bus, star and ring.

Understand how a star can behave like a bus (i.e. hub functionality).

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.

Cisco contrasts between **switches** (function in hardware, is fast & has many ports) and **bridges** (functions in software, is slow & has few ports).

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.

Store and forward switching reads the entire Ethernet frame and checks the CRC before forwarding it out the destination port.

Cut through reads the destination Ethernet MAC address and then immediately forwards the frame out the destination port.

Cut through can change to store and forward when there are lots of errors this is known as **adaptive cut through**.

Fragment free looks at the first 64 bytes of a frame to confirm that no collisions have occurred before forwarding the frame out the destination port.

Fragment free is also known as modified cut-through

The 3 problems associated with layer 2 redundant paths are:

Database instability
Multiple frame transmission
Broadcast storms

Configure a management vlan

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

Configure default gateway

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

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 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)
```

Microsegmentation is place one unique device on each port of a switch.

A link can be in full duplex when there is only one host (device) per switch port.

Microsegmented switches (full duplex links) provide dedicated communications between devices, increased bandwidth and multiple simultaneous conversations. Furthermore, a Microsegmented switch provides media rate adaptation.

Wireless LANs (WLANs) – use the Carrier Sense Multiple Access with Collision Avoidance (CCMA/CA) and operates in half duplex mode.

Compare the popular WLAN technologies

802.11a	802.11b	802.11g
54Mbps throughput	11Mbps throughput	54Mbps throughput
5 Ghz carrier frequency	2.4Ghz carrier frequency	2.4Ghz carrier frequency
Up to 23 channels	Up to 3 channels	Up to 3 channels
Less interference than b or g	More interference than a	More interference than a
Not compatible with b or g	Compatible with g	Compatible with b
OFDM Modulation*	DSSS Modulation**	DSSS* & OFDM**

* Orthogonal Frequency Division Multiplexing

**Direct Sequence Spread Spectrum

Wireless Privacy - Three protocols can be used: WEP (not recommended), WPA (home use) or WPA2 (corporate use).

SSID – Service System ID Wireless: Access Points broadcast an SSID that clients use to identify and associate with access points.

Understand the Cisco 3 layer design model

Core layer (Backbone): Responsible for transporting large amounts of traffic reliably and quickly. It's only purpose is to switch traffic as fast as possible (speed and latency are factors). An example would be a Large ISPs running Cisco 12000, 7500, 7200.

Distribution layer: The distribution layer provides policy-based connectivity, determines fastest/best path to send data to the Core layer. Implement security and QoS at this layer. An example would be routing between regions in an enterprise using a Cisco 3600, 4500, or 4700.

Access layer (Desktop): Controls local end user access to network resources. An example would be switches and routers used by end users to access the network like a Cisco 2950 switch or a Cisco 2600 router.

Know the IP v4 header fields:

The **Version** nibble identifies if this is IP 4 or IP 6.

TOS Type of Service field is how the datagram should be used to be for 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

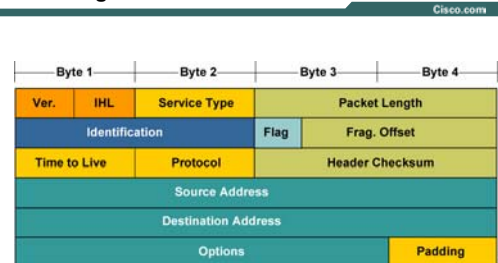
Protocol – identifies the Layer protocol being carried by IP, common protocols include: 6 (TCP), 17 (UDP), 1 (ICMP) and 88 (EIGRP)

Source & Destination addresses are 32 bit hierarchical addresses

Internet Control Message Protocol (ICMP) is used to announce network errors, announce network congestion, announce Timeouts and assist with troubleshooting. It is defined in RFC 792.

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.

IP Datagram Header



© 2004 Cisco Systems, Inc. All rights reserved.

WTR0-020-017

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.

ARP is used by a networked machine to resolve the hardware location/address of another machine on the same local network. ARP is defined in RFC 826.

An ARP table is a cache of MAC address to IP address associations. In Windows, the arp table can be viewed with the command "arp -a"

DHCP (Dynamic Host Configuration Protocol) 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.

BOOTP is older than DHCP and was designed for manual pre-configuration of the host information in a server database, while DHCP allows for dynamic allocation of network addresses and configurations to newly attached hosts. Additionally, DHCP allows for recovery and reallocation of network addresses.

RARP (reverse ARP) is a protocol used by diskless work stations that allows a computer to find out its own IP number based on it's Mac address. Unlike DHCP and BOOTP, a RARP server can only serve a single LAN.

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 13 "authoritative" DNS servers.

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.

Understand IP address structure (dotted decimal) xxx.xxx.xxx.xxx

Identify 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

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

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

Identify 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.

Calculate subnet masks – use my “Eight steps to subnetting success”

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).

Transport layer: Session multiplexing, segmentation, flow control, and reliability

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), Telnet (23), SMTP (25) DNS (53) and WWW (80)

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

Know the structure of **UDP and TCP headers**

16-bit source port		16-bit destination port	
32-bit sequence number			
32-bit acknowledgement number			
4-bit header length	resv	n s w r e	c e u a p r s f i n n
16-bit TCP checksum		16-bit urgent pointer	
Options			
Data			

TCP fields:

Source & Destination ports

Sequence number

Acknowledgement number

Syn, Fin & 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”.

The process of ending a TCP connection

The source PC sends a TCP packet to destination PC with the FIN bit set to 1 – This is interrupted as “can we stop talking?”.

The destination PC receives the FIN packet and responds with a packet that has the FIN and ACK bits set to 1 – This is interrupted as “OK, let's shutdown”.

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 shutdown”.

TCP flow control (sliding window sizes) – the receiver controls the 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.

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

DTE: Data Terminal Equipment (source or destination of network signals)

DCE: Data Circuit-terminating Equipment (convert signals for transmission)

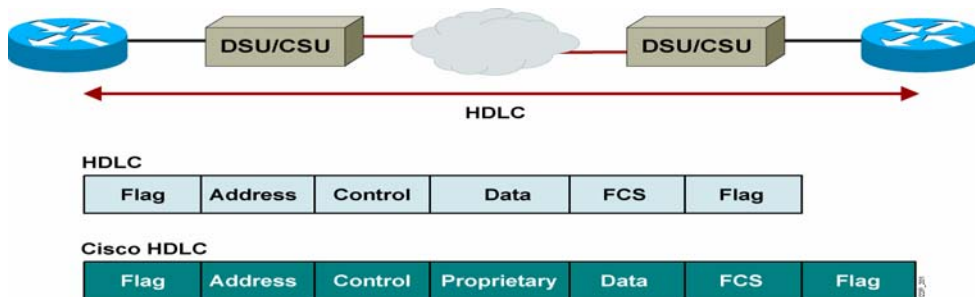
TDM (Time Division Multiplexing) All of the Bandwidth – some of the time

FDM (Frequency Division Multiplexing) Some of the Bandwidth – all of the time

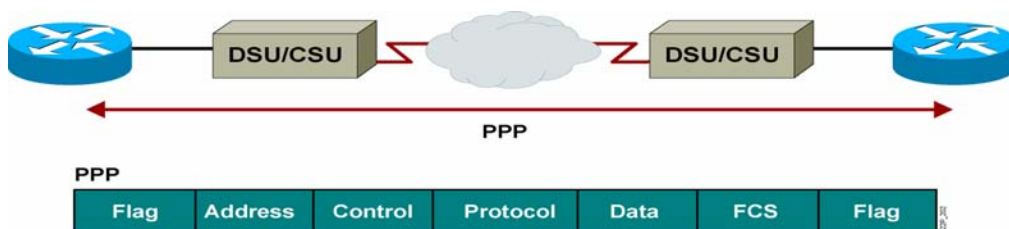
Statistical Muxing – Store & Forward switching, useful with bursty traffic

HDLC is used in Point To Point environments, is open source, simple, but only supports a single layer 3 protocol

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.



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

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

ATM (Cell) – Virtual circuits, fixed sized cells (53 bytes, 48 bytes payload/5 bytes overhead) rock solid error correction.

DSL – a transport technology typically using ATM as it's layer 2 protocol.

ADSL – Asymmetric DSL used for consumer internet access

SDSL – Symmetric DSL used for business internet access

DSLAM – Digital Subscriber Lines Access Multiplexer – Located in the CO provides DSL access for many customers

Cable Modem – by effectively moving the “head end” closer to the customer, more bandwidth is made available. This bandwidth is used to provide internet access.

VPN – By encrypting traffic between two nodes customers use the internet as a WAN.

3 basic steps of startup – **POST (Power On Self Test)**, **Load IOS** and **load config**

The **5 sources** of configuration information: Console port, AUX port, VTY, TFTP, Web

The **2 IOS modes**: User and Privileged

Know that an **amber** 2950 System LED means **POST error**.

2950 LEDs

If the RPS led is off then RPS is off or is not installed.

If the RPS led is green then the RPS is connected and ready to provide back-up power.

If the RPS led is flashing green then the RPS is providing power to another device.

If the RPS led is Solid amber then the RPS is in standby/fault condition.

If the RPS led is flashing amber then the internal power supply in a switch has failed, and the RPS is providing power to the switch.

PORT LED in port status mode (off = no link, green = link present, green flashing = data activity, alternating amber/green link errors, amber the port has been disabled {security/STP})

PORT LED in Bandwidth mode shows switch utilization on a logarithmic scale

PORT LED in Full duplex mode – green = full duplex, off = ½ duplex

PORT LED in speed mode – green = 100 Mbps, off = 10 Mbps

Configure a management vlan

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

Configure default gateway

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

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 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)
```

KNOW THESE PROMPTS

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)#**

“**#show version**” displays the IOS version/file, the configuration register, device up time and the hardware platform (revision/ram)

“**#show interfaces**” displays all the interfaces on a box, their status, and Layer 2 protocol information

“**#show running-config**” displays configuration info including passwords, ip addresses, routing protocols and more.

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

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

Save device configuration: #copy running-config startup-config”

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

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 version 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

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

To **enter the configure interface mode** enter the global configuration mode and then enter the command interface with the interface nomenclature.

```
#configure terminal  
(config)#interface Serial1/1
```

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 determine if an interface is DTE or DCE use the **show controllers** command

```
#show controllers serial 1/1
```

To assign a clock rate to a serial interface use the **clock rate** command

```
(config-if)#clock rate 64000
```

The **show interfaces 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.

```
#show interfaces serial 1/1  
#Serial 1/1 is up, line protocol is up
```

Bouncing an interface will clear many problems –

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

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

#show cdp neighbors – device ID, platform, local and connected interfaces and capabilities

#show cdp entry “device ID” or “*” will show neighbor IP address

#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)

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 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)

Configuration register 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 (**Ctrl+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 flash displays the size of the IOS file, total memory and free memory

#copy running config is a merge to the running configuration

#Show is static w/low over head

#debug is dynamic with high overhead

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

Interior Gateway Protocol – RIP, OSPF, IGRP, EIGRP, IS-IS

Exterior Gateway Protocol – BGP4

3 classes of routing protocols

Distance vector (RIP, RIPv2)

Link State (OSPF, IS-IS)

Hybrid/Advanced Distance vector (EIGRP)

Characteristic	RIPv1	RIPv2	IGRP	EIGRP*	IS-IS	OSPF
Distance vector	X	X	X	X		
Link state					X	X
Automatic route summarization	X	X	X	X		
Manual route summarization		X		X	X	X
VLSM support		X		X	X	X
Proprietary			X	X		
Convergence time	Slow	Slow	Slow	Very Fast	Fast	Fast

* EIGRP is an advanced distance vector protocol with some link features.

Administrative Distance is and 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**

When a router is running a classful routing protocol, a routers discards packets to unknown subnets of directly connected networks. The “**IP classless**” command forwards these packets to the next hop.

RIP networks trade routing tables every 30 seconds, the default hold down timer is 180 seconds, and RIP only load balance over equal paths (4 by default/6 maximum)

RIP v1 is classful, does not advertise subnet masks and is not password protected.

RIP v2 is classless, advertises subnet masks and is password protected.

Configure RIPv2:

```
(config)#router rip
(config-router)#version 2
(config-router)#Network x.x.x.x
```

Inter Connecting Network Devices (ICND) 2

ALL CONCEPTS IN ICND 1 ARE TESTABLE FOR ICND 2 OR THE CCNA

Static VLANs assign a VLAN to a port or ports

Dynamic VLANs associate MAC addresses and VLANs through VMPS (VLAN Policy Membership Server) and are not frequently used

Access ports support a single data VLAN and **trunks** support multiple VLANS

Best practice – one subnet per VLAN

Voice VLAN (aka Auxiliary VLAN) - a 2nd VLAN assigned to an access port

VLANs; segment networks, reduce broadcast traffic, provide security and are used when implementing QOS

802.1q is standards based tagging.

ISL (advantages and disadvantages)

Native VLAN allows non-vlan members to participate in LAN – usually vlan1 – untagged

VLAN Trunking Protocol (VTP) distributes a VLAN database throughout the network

VTP has 3 modes:

Client - receives & propagates VTP advertisements but cannot create/change

Server – create, receives & propagates VTP advertisements can reate/change

Transparent – creates local VLANS only forwards VTP advertisements

VTP pruning, when enabled, reduces unnecessary flooded frames

Configure vtp mode, domain name, password & pruning

```
(config)#vtp mode [ server | client | transparent ]
```

```
(config)#vtp domain domain-name
```

```
(config)#vtp password password
```

```
(config)#vtp pruning
```

```
(config)#end
```

Put an interface in trunk or access mode:

```
(config-if)# switch port mode (trunk| access)
```

Some switches support dynamic trunk configuration. The **trunk** option makes the port a trunk. The **dynamic desirable** option makes the port a trunk IF the other end is configured as a trunk OR dynamic desirable OR dynamic auto. The **dynamic auto** option makes the port a trunk IF the other end is configured as a trunk OR dynamic desirable.

```
(config-if)# switch port mode (trunk| dynamic desirable| dynamic auto)
```

To create a vlan

```
(config)#vlan 2  
(config-vlan)#name xxxx
```

To assign a vlan to a port:

```
(config)# fa 0/2  
(config-if)#switchport mode access  
(config-if)# switchport access vlan2
```

To verify VTP configuration

```
#sh vtp status
```

The **show interfaces fa0/11 trunk** command verifies trunking and vlan configuration

#show vlan command displays all ports a vlan is connected to.

Etherchannel – combines multiple ports into one channel

Spanning tree protocol (802.1d) provides loop free redundant topology.

A **Bridge ID** 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

All ports on a root switch are **designated**

All ports that are not designated and not root are blocked

Know the four states a spanning tree port transitions through

Blocking (receives BPDU's, but 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

Rapid Spanning Tree Protocol (802.1w) quickly moves edge ports and point-to-point links to the port forwarding state.

Rapid Transition to Forwarding aka Port Fast – is used to implement Rapid Spanning Tree Protocol.

BPDUs are transmitted every 2 sec by default

If no BPDU is received before the **max age** timer expires then spanning tree is recalculated. Max age is set to **20 seconds** by default.

Common Spanning Tree (CST) is an IEEE protocol and does not allow load balancing between vlans

Per VLAN Spanning Tree (PVST+) protocol is Cisco proprietary, provides load balancing, but is more taxing to the CPU than CST

Configure portfast on a port

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

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

Configure a switch as root for a VLAN 1

```
(config)#spanning-tree vlan 1 root primary
```

Configure "router on a stick" for 802.1q

```
(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
```

802.1x is IEEE standard for port based authentication

Be familiar with switch, VTP and VLAN troubleshooting procedures

Techniques used by Distance Vector protocols to prevent routing loops

Split horizon - It is never useful to advertise information about a route back in the direction from which the original information came.

Route poisoning - advertise a distance of infinity for networks that have gone down

Poison reverse - when a router receives a “poison route” to sends back a “poison reverse” which acts like an acknowledgement (the exception to split horizon).

Hold down timers - prevents route flaps by rejecting updates for a period of time. The only exception – routers will accept updates for BETTER routes.

Triggered updates - don't wait for scheduled periodic updates – update as soon as a topology change is detected.

Distance Vector protocols prevent “**count to infinity**” by defining a maximum hop count.

Link state protocols break an autonomous system into sub-networks called “Areas”. If multiple areas exist they must travel through area 0/

Link State Advertisements (containing Router ID, interface and Bandwidth) are flooded to all routers in an Area. The routers use Dijkstra's algorithm to calculate routes with the least cost to each network.

Link state protocols **converge more quickly** and **use less bandwidth** than distance vector protocols.

Link state protocols use **more memory** and **processor resources** than distance vector.

Variable-Length Subnet Masks (VLSM)

VLSM enables a router to **support more than one** subnet mask size and provides a more efficient way to allocate IP addresses

Understand that VLSM subnets **can not overlap**

Route summarization represents multiple networks as a single entry in the routing table

Discontiguous networks can not be summarized with a single routing table entry

OSPF is a link state protocol

OSPF forms a neighbor relationship with directly connected routers by exchanging hello packets.

Hello packets contain:

- Router ID
- Area ID
- DR Address
- BDR Address

Link State Advertisements (LSAs) are flooded to all routers (IP Address 224.0.0.5)

OSPF uses the **shortest path first (Dijkstra)** algorithm to calculate best path

Cost = 100,000,000/BW in bps (T1 is about 66.66)

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

Configure OSPF:

```
(config)#router ospf 100
(config-router)#Network 10.0.0.0 0.255.255.255.0
```

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

An **Area Boarder Router (ABR)** attaches to the backbone area and one other area

In multiaccess networks (networks with more than 2 routers), 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.

Router ID is based on the highest IP address of any interface. The DR is elected (in part) based on the highest router ID. **A loop back address** allows you to assign a stable router ID

OSPF load balances across equal paths only.

Path cost can be manually configured – **(config-if)# ip ospf cost <value>**

Plain text Authentication

```
(config-if)# ip ospf authentication
(config-if)# ip ospf authentication-key password
```

#show ip ospf neighbors displays the neighbor table for EIGRP

#show ip ospf database displays topology or an area

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

#show ip protocols commands to verify ospf configuration

#debug ip ospf events shows ospf neighbor exchanges

Be familiar with OSPF troubleshooting procedures

EIGRP is an advanced distance vector protocol

3 tables maintained

EIGRP Neighbor Table – lists directly connected routers

EIGRP Topology table – list all EIGRP routes

Routing Table – list best routes

Successor route – the best route to network

Feasible successor – alternate routes to the network

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)
Diffusing Update Algorithm (DUAL) picks a successor & feasible successor route
EIGRP supports multiple protocols w/ 3 tables for each protocol (neighbor, topology, routing)

Configure EIGRP:

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

No **auto summary** command enables support for VLSM

#show ip eigrp neighbors displays the neighbor table for EIGRP

#show ip eigrp topology displays networks, distance and feasible

#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

(config-router)#variance multiplier command allows load balancing across unequal paths

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

MD5 Authentication

```
key chain RouterXchain
key 1
key-string firstkey
accept-lifetime 04:00:00 Jan 1 2006 infinite
send-lifetime 04:00:00 Jan 1 2006 04:01:00 Jan 1 2006
key 2
key-string secondkey
accept-lifetime 04:00:00 Jan 1 2006 infinite
send-lifetime 04:00:00 Jan 1 2006 infinite
<output omitted>
!
interface Serial0/0/1
bandwidth 64
ip address 192.168.1.101 255.255.255.224
ip authentication mode eigrp 100 md5
ip authentication key-chain eigrp 100 RouterXchain
```

Be familiar with EIGRP troubleshooting procedures

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**

Special purpose ACL's include: **Dynamic ACLs** (aka Lock-and-Key) provides authentication for network users, **Reflexive ACLs** allow inbound traffic ONLY if an inside host initiated communication, **Time-Based ACLs** allow access based on time/day

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 deny 192.168.3.0 0.0.0.255  
(config)# access-list 10 permit any
```

Know the structure of an access-list that blocks only 192.168.3 network from www access

```
(config)# access-list 101 deny tcp 192.168.3.0 0.0.0.255 any eq 80  
(config)# access-list 101 permit ip any any
```

To apply an access list in the outbound direction of physical interface use this structure

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

To apply and access to the inbound direction of a vty interface use this command:

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

(config)#no access-list xxx removes the ACL from the router

(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

#show access-list xxx shows an acl content

#show ip interfaces verifies acl placement

Network Address Translation (NAT)

NAT benefits simplifies management, conserves address space and improves security

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 an 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

Port Address Translation maps multiple inside local address to a single inside global address. The L4 port addresses are used to keep track of the individual translations

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

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

Leading zeros are optional.

Once in an address, a string of zeros can be compressed to ::

IP v6 address types:

Global IP addresses assigned by IANA beginning with 2000::/3

Private Addresses begin with FE80::/10

Site local – like private addresses in IPv4. These addresses are routable, but only within the site network. Begins with; FEC, FED, FEE and FEF

Link local – NOT routable – valid on a local link only! FE8, FE9, FEA and FEB

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

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

Global IP addresses can be assigned in 2 ways

Static (Manual & EUI-64)

Dynamic (Stateless & DHCPv6)

IPv4 to IPv6 transition can be accomplished by:

Running a dual stack

Tunneling one protocol across another

Network Address Translation - Protocol Translation (NAT-PT)

Apply an IP v6 address to an interface

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

Configure RIPng

```
(config)#ipv6 unicast-routing  
(config)#ipv6 router rip TEST  
(config)#int fa 0/0  
(config-if)#ipv6 address 2001:dd45:c77:2::/64 eui-64  
(config-if)#ipv6 rip TEST enable
```

There are two types of VPNs

Site-to-Site VPN

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

Symmetric Key Cryptography uses one secret key shared by both parties

Asymmetric Cryptography uses one key that can only encrypt data, but can not decrypt data, and a second key that is used to decrypt that data.

Symmetric Key algorithms include: DES, 3DES and AES

RSA is an **Asymmetric Key** (Public Key) algorithm

IPsec uses the **Authentication Header (AH)** to provide authentication [the identity of the sender] and to ensure the integrity of the data [no changes to the data] – but does not provide confidentiality.

IPsec uses the **Encapsulating Security Payload (ESP)** to provide authentication.

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

(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

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 receives 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.

Sub interfaces are used to solve the split horizon issues with NBMA

NBMA 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
```

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
```

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

FRF .5 defines Frame Relay across ATM

FR .8 defines Frame Relay translation to ATM

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