Inter Connecting Network Devices (ICND) 1

This is my personal summary of what I believe to be the key points of needed to pass Cisco's ICND 1 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 ICND 1 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.

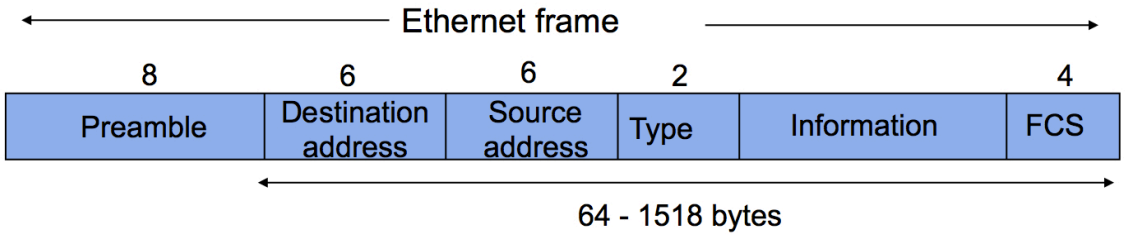
Ethernet

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**.

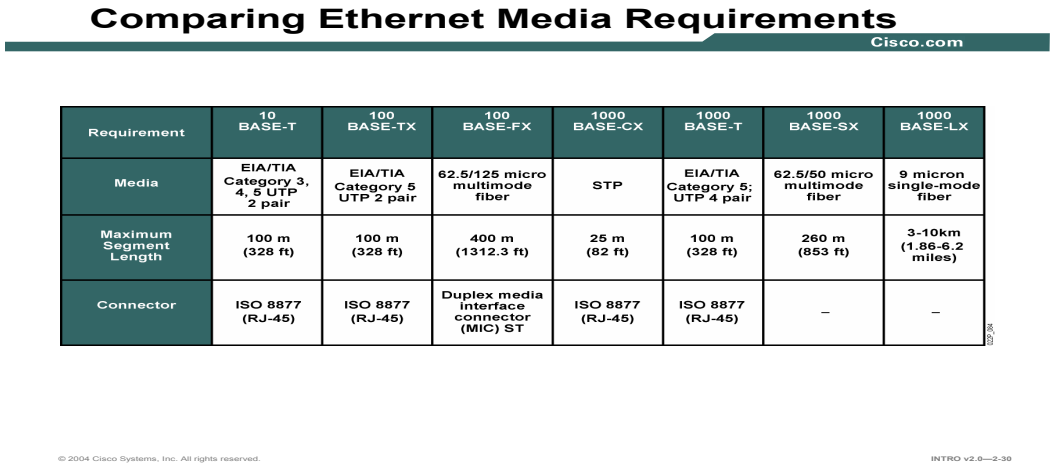


Understand straight through and crossover cables.

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:

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)

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

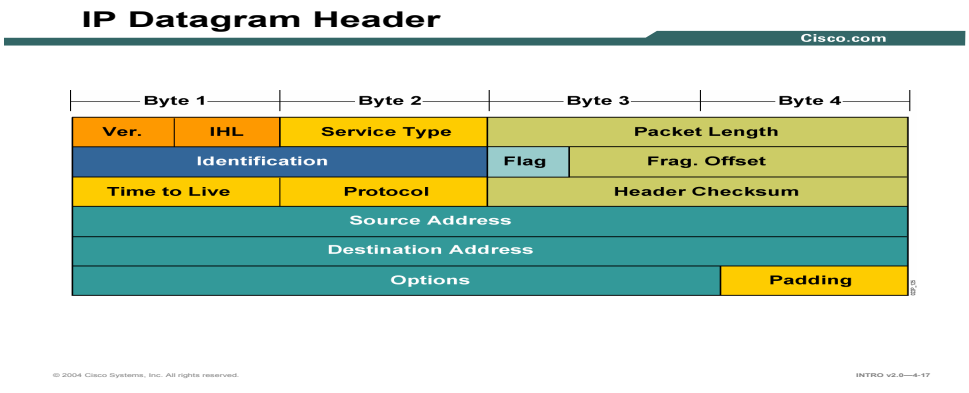
Define the following terms that are associated with the show interface status command:

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.

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) 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.

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.

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 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 (Host & Network 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**.

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)

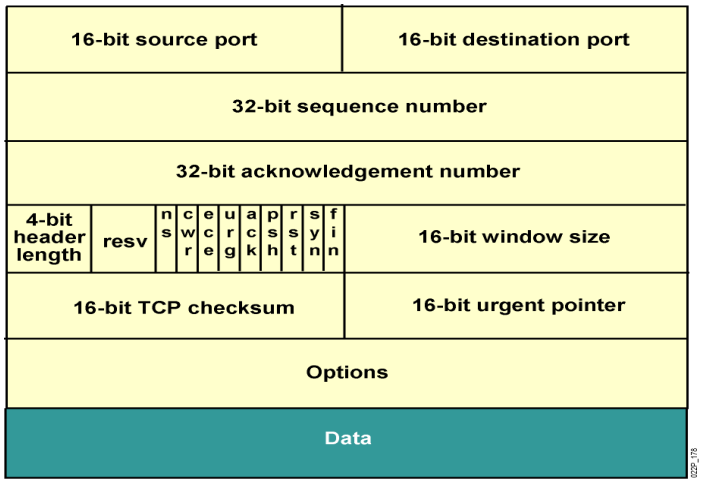
TCP characteristics: Connections, full duplex, error checking, sequencing and acknowledgements, flow control packet retransmission

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, 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.

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. 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." - 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

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

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.

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 access-list that blocks only 192.168.3 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 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

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 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

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

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

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**

Configure a DHCP Relay Agent on an interface: **(config-if)# ip helper-address x.x.x.x**

DTP (Dynamic Trunking Protocol) is a Cisco proprietary used to automatically establishes a trunk between two connected Cisco switches.

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

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

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 ann **Exterior Gateway Protocol** – BGP4

Know about a single area OSPF network

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
Hello/Dead Interval
Authentication data

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

Link State Advertisements (LSAs) are flooded to all routers (Multicast 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)

Link state protocols use **more memory** and **processor resources** than distance vector. To compensate for this **Link state** protocols break an autonomous system into sub-networks called "Areas". If multiple areas exist they must travel though area 0

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

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.

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

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

Each OSPF router has a unique number called a Router ID. The highest IP address on the router is chosen, unless there is a loopback address. If a loopback address exists this becomes the Router ID unless router-id command has been used. The **router-id** command takes precedence over all other methods of ID assignment.

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

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

show ip protocols displays the current configuration of OSPF

show ip route displays the contents of the routing table

show ip int brief displays all the interfaces on this router enabled for OSPF

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

Know the following facts about IPv6:

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

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.

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).

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

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

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

IPv6 static routes are configured similarly to IPv4 static routes

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

OSPFv3 is a link state protocol for IPv6

The router ID has the same 32 bit format as OSPF for IPv4

Adjacencies and next hop information use the link-local addresses

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 ipv6 ospf 1 area 0