CCNA 640-507

Study Notes

Written by Frédéric Demers, CCNA

7 Jan 2002

These notes were taken based on the information contained in several books and internet sources but mainly Sybex's CCNA Cisco Certified Network Associate Study Guide, by Todd Lammle, and Sybex's CCNA Exam Notes, by Todd Lammle and Sean Odom. The information in this guided is structured based on the organization of the first book.

The information following is very condensed and additional study material is a definite must. I mostly succeeded capturing the information of each chapter on a single page (I removed the Dial-on-Demand Routing because it's also removed from the exam notes). I also recommend the use of a Router Simulator unless you can use an actual router. I used the Boson Router Simulator, and I must say that a lot of commands are not supported, but the updates are frequent.

Good Luck…

Table of Contents:

Note on the syntax used in these study notes:

The syntax used for IOS commands is the following:
command [**optionalKeyword**] **choice1Keyword**/**choice2Keyword** *parameter*.

Bold typeface indicates a Cisco IOS keyword and must be entered as is. Information in square brackets is optional, used for different configuration options. Italic represent parameters such as minutes, seconds, numbers. Parenthesizes are also used to group options together such as:

command (choice1Keyword *bps*)/(choice2Keyword *kbps*)

where you can either type the first keyword and its associated parameter, or the second keyword and its associated parameter. Note that you must enter either or, as no information is surrounded by square brackets.

Examples:

show ip/ipx route: either **show ip route** or **show ipx route**
terminal [**no**] **editing:** either **terminal editing** or **terminal no editing**
show cdp [(**neighbor** [**detail**])]: either **show cdp, show cdp neighbor** or **show cdp neighbor detail**

See Part IX - Access Lists for funky examples…

Typing in **cl**? will give you all the commands starting with cl, whereas typing **clock** ? will display all options associated with the keyword.

Part I – Internetworking

ISO's(International Organization for Standardization) OSI (Open Systems Interconnection) Model:

	Layer	PDUs	Remarks, Examples
7	Application		WWW, E-mail **gateways**, user interface. Also responsible for understanding the resources needed to communicate between two devices and establish their **availability**. SMTP, FTP.
6	Presentation		Translates and converts data into a known format such as ASCII, JPEG, MIDI, MPEG, encryption, compression. The only layer that can actually change data.
5	Session	Data	Keeps different applications' data separate, **NFS, SQL, RPC, NetBIOS names, X Window**. Offers three modes – full-duplex, half-duplex and simplex. Maintains communication channels and provides dialogue control. Managing, setting up and tearing down sessions.
4	Transport	Segments	Reliable or unreliable delivery, error correction before retransmit, TCP/UDP. Performs flow control, end-to-end connection. **Port numbers** are used at this layer. **Multiplexing**, teardown of virtual circuits. Reassemble the data stream.
3	Network	Data and Route Update **Packets** or Datagrams	Logical addressing, routing, IP and IPX. Route update packets are sent at this layer, in addition to the data packets. Layer 3 devices such as **routers** break up broadcast domains and collision domains.
2	Data-Link	Frames	Layer 2 devices such as **switches** or **bridges** break up collision domains whereas hubs do not. Uniquely identifies each device on a local network. This layer uses **service access points,** identify network layer protocol used, flow control and sequencing of control bits (LLC – Logical Link Control - sublayer) and deals with the protocol access to the physical medium, network topology and error detection/notification (MAC – Media Access Control - sublayer). A MAC address on a NIC (Network Interface Card) is a 48 bits address formatted in 12 hexa digits grouped in twos as such: AF-98-C0-72-A3-2B
1	Physical	Bits	Moves bits between devices, specify voltages, wire speed and pin-out cables. **Hubs** are also known as multi-port **repeaters** and operate at this layer.

A layered model enables different vendors' products to interoperate ("plug-n-play"), breaks a complex problem into more manageable entities, eases the changing of one layer without changing the other. Realize that breaking up a collision (or broadcast) domain creates **more** collision domains.

Cisco Hierarchical Model:

Layer	Examples
Core	Large amounts of traffic reliably and quickly. Fault tolerance important. Don't use VLAN, access lists or packet filtering at this layer. Cisco recommends using layer 2 switches at this layer.
Distribution	Provides routing, filtering and WAN access. Place to implement policies on a network (packet filtering, access lists, queuing, security and network policies, address translation, firewalls, redistribution between routing protocols, static routing, routing between VLAN and other workgroup support functions, definition of **broadcast** and multicast domains. Cisco recommends using routers at this layer.
Access	Continued access control and policies from the distribution layer, creation of separate **collision** domains (and **segmentation** of contention networks). Cisco recommends using layer 2 switches at this layer.

IEEE Ethernet (MAC) Standards:

IEEE Number	Standard
802.3	Ethernet
802.3u	Fast Ethernet Uses MII (Media Independent Interface) and transmits using nibbles (4 bits at a time)
802.3z	Gigabit Ethernet Uses GMII (Gigabit MII) and transmits 8 bits at a time.

Ethernet Physical Media (created by Digital Equipment, Intel and Xerox):

10Base2	Thinnet 50-ohm coax 185m, 30 hosts per segment Physical and logical bus with AUIs	100BaseFX	Fiber cabling 62.5/125-micron multimode fiber point-to-point, 400m ST or SC connectors
10Base5	Thicknet 50-ohm coax 500m and 208 hosts per segment Physical and logical bus with AUIs	1000BaseCX	Copper shielded twisted-pair 25m
10BaseT	EIA/TIA cat 3,4 or 5, using two-pair unshielded twisted-pair (UTP) wiring. 100m and 1 user per segment Physical star and logical bus with RJ-45	1000BaseT	Cat 5, four-pair UTP wiring, 100m
100BaseTX	EIA/TIA cat 5,6 or 7 UTP two-pair wiring 100m and 1 user per segment physical star and logical bus with RJ-45 MII	1000BaseSX 1000BaseLX	Multi-mode fiber 62.5/50-micron, 260m Single-mode fiber 9-micron core, 10km

Straight-through vs crossover cables (wire 1<-> wire 3, wire 2<-> wire 6):
Considering the devices grouped in two categories: 1-switches / hubs / bridges, 2-workstations / servers / routers
If changing category, use a straight through cable, else use a crossover cable. (or use straight-through when one of the port is marked with an X)

Ethernet Auto-Negotiation: determines the link speed and duplex status.
Ethernet Frames:
Ethernet II – uses a two-byte type field instead of the length.
802.3 – cannot identify the upper-layer protocol
802.2 (802.3 with LLC information in the data field of the header) – able to identify the upper layer protocol
SNAP – Subnetwork Access Protocol – used in AppleTalk and Cisco Discovery Protocol)

Half-Duplex: contention net using CSMA/CD (Carrier Sense Multiple Access/Collision Detection) and a backoff algorithm when collision occur.
Full-Duplex: two communication paths are required and compatible full-duplex NICs. Loopback and collision detection must be disabled. Sets up a point-to-point connection with the remote device. There are no collisions on a Full-Duplex link.

Ring LAN:
Token Ring: standard created by IBM and reflected in IEEE 802.5 with speeds of 4 or 16 Mbps. Stations cannot transmits until they have the token, which they can reserve using the Reservation Bits.
FDDI (Fiber Distributed Data Interface): token-passing ANSI standard providing LAN speed of up to 200 Mbps if dual rings are active. Only LAN topology that is both physical and logical ring.
MSAU: MultiStation Access Unit, the controller of the token ring LAN, for up to 8 stations.
NAUN: Nearsest Active Upstream Neighbour
Active Monitor: one station on the ring always ensures there is only ever one token on the ring.
Beaconing: process by which a station attempts to determine a network failure.

Part II – Switching Technologies

Switch Functions:
Address Learning: when a host transmits a frame, it's hardware address is recorded in the MAC Address Table, along with the port the frame has been received on.
Forward/Filter Decisions: If the address is unknown, the frame is forwarded to all ports except the one on which the frame was received. In other cases, the frame is only sent to the appropriate interface.
Loop Avoidance: Loops occur when there are multiple links between switches. A broadcast storm occurs when two switches constantly rebroadcast the same frame. Devices may receive the same frames several times, and from different origins. The same problem can cause MAC Address Table confusion (called trashing) if the device is a switch trying to determine the entry port of a MAC address. These problems can be avoided by the Spanning Tree Protocol (STP).
Bridges are software based and can only have one Spanning Tree instance, switches are hardware based (ASIC – Application Specific Integrated Circuit) and have lower latency.

Spanning Tree Protocol (STP): Standard IEEE 802.1d that uses the STA (Spanning Tree Algorithm) to prevent network loops.
Bridge Protocol Data Units (BPDUs): packets of information exchanged between switches to support the STP. They are sent every 2 seconds by default. MaxAge is a timer indicating how long before the bridge should wait before concluding the topology has changed.
Bridge ID: composed of a priority from 1 to 32768 (default) and the MAC address of the bridge, this is communicated using BPDUs.
Root Bridge: elected by the lowest bridge ID. The ports on the Root Bridge are **Designated Ports** (forwarding) and if the route bridge is not connected to the redundant link, the one determined by the lowest-cost link (or bridge ID in the event of a tie) will be a designated port. All other switches will have non-designated ports onto the redundant link (blocking).
Root Ports: ports linking to the Root Bridge in non-root bridges. They are determined by the lowest-cost path to the Root Bridge.
Blocked Ports: Ports other than the root port that will not forward frames, but will still receive BPDUs.

Port States:
Blocking: does not forward frames, but listen to BPDUs. All ports are in blocking state by default when a switch is powered up.
Listening: Listens to BPDUs to ensure no loops occur on the network before passing data frames.
Learning: Learns MAC addresses and builds a filter table but does not forward frames.
Forwarding: Sends and receives all data on the bridged port.
Disabled: No frame forwarding or BPDUs are sent or received.

Convergence: transition time from blocking to forwarding state to allow the device enough time to learn the latest network topology (**default is 50 seconds**). When a switch determines a blocked port has to be activated due to a down-link, the port will first go into **listening** mode to ensure no loops will be created.
Latency: time elapsed between the receiving of a frame and its forwarding.

LAN Switch Types:
Store-and-forward: The complete frame is received, checked, and then forwarded. Unchangeable default on Catalyst 5000 switches.
Cut-through: Only the destination hardware address is looked up and the frame is then forwarded.
FragmentFree or **modified cut-through**: Default for Catalyst 1900. Checks for the first 64 bytes in the data field of a frame before forwarding it.
Both **Cut-through** and **FragmentFree** have fixed latency, and **Store-and-Forward** has variable latency.

Part III – IP

DOD TCP/IP Model:

Layers	OSI Model	Protocols (Port or protocol numbers)	Definition
Process	Application Presentation Session	Telnet (23) FTP (21) TFTP (69) SMTP (25) SNMP (161) DNS (53) BootP NFS DHCP HTTP (80)	Telephone Network - terminal emulation File Transfer Protocol – file transfer that also allows authentication, directory browsing Trivial File Transfer Protocol – stripped down FTP used to backup and restore routers' config Simple Mail Transfer Protocol – used to send email. POP3 (110) and IMAP (143) retrieve mail Simple Network Management Protocol – collects valuable network info by polling devices (UDP) Domain Name Service – resolves domain names into IP addresses Bootstrap Protocol – used in diskless stations that receive network info and OS from the server Network File System – allows different file system to interoperate. Uses UDP. Dynamic Host Configuration Protocol – enhanced from BootP, can provide IP, subnet, domain, gateway, DNS and WINS information. **Uses UDP.** Hyper Text Transfer Protocol – WWW protcol
Host-to-Host	Transport	TCP (6) UDP (17) NBP	Transmission Control Protocol – connection-oriented protocol using windowing as flow-control mechanism. Segments are numbered and the number of the last segment received is sent back in the acknowledge message. User Datagram Protocol – unreliable connection-less protocol that has less overhead than TCP. Port numbers: used by TCP and UDP. Numbers 0-1023 are well-known port numbers. Numbers 1024 to 65534 can be used by a transmitting host to initiate the communication. Name Binding Protocol – AppleTalk protocol that matches logical device names to address.
Internet	Network	IP ICMP (1) ARP RARP Routing	Internet Protocol – four-byte number used to route packets on the internet. Connectionless Protocol Internet Control Message Protocol – management protocol and message svc provider for IP. Used in "destination unreachable", "buffer full", "hop limit" messages, and in **ping** and **trace**. Implemented by all TCP/IP hosts. Address Resolution Protocol – retrieves a MAC address from an IP address Reverse Address Resolution Protocol – retrieves an IP address from a MAC address All routing protocols operate at this layer
Network Access	Data-Link Physical		Ethernet, FastEthernet, Token-Ring, FDDI

IP Addressing:

Classes: (n is the network address portion, and h is the host address portion)		Reserved Addresses:
Class A: n.h.h.h, n ∈[0,127] (starts with 0) Class B: n.n.h.h, n ∈[128.0,191.255] (starts with 10) Class C: n.n.n.h, ∈[192.0.0,223.255.255] (starts with 110) Class D: multicast Class E: research	private: 10/8 private: 172.16/12 private: 192.168/16	Network address of 0s : this network or segment Network address of 1s : all networks Host address of 0s : this host Host address of 1s : all hosts Address of 1s : all nodes on current network - flooded broadcast Address of 0s : used by Cisco to designate the default route Address 127.0.0.1 : this node used for loopback tests.

IP Subnetting:

Information	Formula	Mask	*number*	Mask	*number*
Subnet address	$y_i=(256-number)*i$	10000000	128	11111000	248
First host	y_i+1	11000000	192	11111100	252
Last host	$y_{i+1}-2$	11100000	224	11111110	254
Subnet broadcast address	$y_{i+1}-1$	11110000	240	11111111	255

$i \in [1, n_s]$

Number of subnets: $n_s=2^{(hostbits-x)} - 2$, – hostbits is the number of bits reserved for the host in that class (8 for class C, …)

Number of hosts: $n_h=2^x - 2$

where x is the number of unmasked bits

It is essential to know how to manipulate subnets to create a given number of hosts or subnets. It is also essential to be able to calculate the broadcast address of a given host or network and subnet mask.

Part IV – Basic IOS Commands

A Cisco router without a startup-config file will enter in the **setup** mode, which you can exit to access the Command Line Interface (CLI). The setup mode offers the Basic Management and Extended Setup. You can enter the setup mode again with the command **setup** at the CLI.

Cursor Commands:

Ctrl+A	start of line	Ctrl+F or ->	forward one char	Ctrl+R	redisplays a line	Ctrl+Z	ends configuration mode
Ctrl+E	end of the line	Esc+F	forward one word	Ctrl+U	erases a line	Tab	completes the command
Ctrl+B or <-	back one char	Ctrl+D or bksp	deletes one char	Ctrl+W	erases a word	Ctrl+P	displays the previous command (like arrow up)
Esc+B	back one word						

Press return to initiate the user EXEC mode: ">" [*whatever*]: indicate that whatever is the default or current option.	**enable/disable:** used to enter or exit the privileged EXEC mode. **logout/exit**: to terminate the session. **exit** goes up one level.

General commands entered in the **"#"** mode:
clock set *hh*:*mm*:*ss d month yyyy*: sets the current time and date.
show history/terminal: shows last 10 commands (**history**) or terminal config and history buffer size (**terminal).**
terminal history size *size*: sets the history buffer size where *size* is between 0-256**.**
terminal no editing: disable or enable the terminal editing keys in the table above.
show version: displays basic IOS and router information, as well as names of config files and boot images, and config register.
show flash: displays the content of the Flash memory, and if only one IOS is in Flash memory, will output the same as **show version**.
show startup-config/running-config: displays current and NVRAM based configuration files.
copy running-config startup-config: used and required to save the current configuration. Reverse to restore.
erase startup-config: resets the router's NVRAM. The router will boot in setup mode next time.
ping/trace/telnet: tools provided to verify connectivity. U=Unreachable, ?=Unknown packet received, .=Time down, P=Unreachable port received.
clear counters *interface*: clears the "show interface" counters on this interface.
show controllers *type number*: information about the physical interface itself. **A space is required between *type* and *number*.**
reload: reboots the router and reloads the startup-config file.
boot system rom/flash *img*: indicate what image the router will use during the next boot.
boot system tftp *img address*: tells the router to use the configuration file *img* from a tftp server at *address*.

config terminal/memory/network: used modify the configuration from the running-config, the startup-config or a from a TFTP server.

Commands entered in the Global Configuration **"(config)#"** mode:
hostname *name*: used to define a hostname that is locally significant only.
enable [**secret**] **password** *password*: sets enable or secret mode password. **secret** will override the non-secure password if set and is encrypted.
[**no**] **service password-encryption**: encrypts or not (**no**) the enable and line passwords.
banner login/motd *char*: sets the login or message of the day banners, where *char* is the delimiting character.

interface *type* [*slot*/]*number*[**.***subinterface*]. You can skip the space between the interface *type* and its *number*. Certain switches equipped with VIP cards use the syntax **interface** *type slot*/*pan*/*number*[*.subinterface*] where *pan* is the Port Adapter Number.
line (**vty** *number number*)/(**aux**/ **console** *number*): used to enter the configuration of the console, aux line or VTY lines (telnet).

Commands entered in the **"(config-if)#"** mode:
description *name*: used to define a description for the interface. *Name* must have underscores rather than spaces. **show run** and **show int 0/***n* will both show the descriptions set on the interfaces.
no shutdown: used and required to bring up an interface. The interface will show as administratively down.
ip address *ipaddress subnetmask*: used to set the IP address and subnet mask of an interface.
clock rate *bps*: sets the clock rate on serial ports.
bandwidth *kbps*: sets the bandwidth of a serial port for routing and STP protocols to establish the best path.

Commands entered in the **"(config-line)#"** mode:
logging synchronous: stops console msgs from overwriting command line inputs.
exec-timeout *min sec*: sets the time-out to *min sec* for the console.
[**no**] **login**: used to set the password when followed by **password** *password*. A password is required on the VTY lines before Telnet can be used by default unless **no login** is used.

Router Memory:
ROM: Read-Only Memory which stores the bootstrap startup program, the power-on self-test (POST) procedures and a baseline IOS. The ROM also contains the ROM monitor, used for manufacturing testing and troubleshooting, and the Mini-IOS, or RXBOOT, which can be used to bring up an interface and load a Cisco IOS into flash memory.
Flash Memory: EEPROM (Electronically Erasable Programmable Read-Only Memory) which stores the IOS (Internetwork Operating System).
NVRAM: Non-Volatile Random Access Memory stores the startup config. A switch has a separate VTP NVRAM which can be deleted with the **delete vtp** command.
RAM or DRAM: Random Access Memory - holds dynamic info such as the current configuration file, the current IOS, caching and buffering.

Part V – IP Routing

Routing: process involving the selection of the best path and the transmission of the data in the chosen direction.

Static Routing: process by which the administrator manually inputs all routing table information.
[**no**] **ip route** *destnet netmask nexthop* [*admindist*] [**permanent**]: *nexthop* is the pingable IP address of the next router or the exit interface for a WAN link. The **permanent** option will keep the route in memory even if the link goes down. Use the **no** keyword to remove a route entered.

Default Routing: by replacing *destnet* and *netmask* with the 0.0.0.0 wildcard, you can configure a default route on a stub network.
ip classless: required when using default routing since Cisco routers expect by default to know the subnet of all remote networks.

Dynamic Routing: process of using protocols to find and update routing tables.

Routing Protocol	Definition	Example Protocols	Default Admin Distances	Maximum Hop Count
		Directly connected	0	
		Static Routing	1	
Distance vector	uses a distance to a remote network to find the best path. Uses hop counts, tick counts (1/18 sec) or bandwidth of links. This type of routing protocol typically has a slow convergence time. Updates are more frequent than link state.	RIP (Routing Information Protocol) IGRP (Interior Gateway Routing Protocol)	120 100	15 255
Link state	maintains three tables (directly attached neighbours, topology of entire network, and routing table)	OSPF (Open Short Path First) – uses the Dijkstra algorithm NLSP (Netware Link State Protocol)	110	
Hybrid	Uses aspects of distance vector and link state.	EIGRP (Enhanced IGRP)	90	224
		External EIGRP	170	

RIP (Routing Information Protocol): RIP only uses hop count and is capable of performing round-robin load balancing to up to six equal-cost links. Pinhole congestion happens when two equal-cost links are of different bandwidth, which is disregarded by RIP. RIP does not support AppleTalk. Routing information messages including the complete routing table are sent every 30 sec by default.

(config)#**router rip**: enables RIP.
(config-router)#**network** *network*: limits the propagation of the RIP messages to the *network*. For example, if subnet 172.16.40.0 is to be used by RIP, then network should be 172.14.0.0.
(config-router)#**passive-interface** *type number*: the interface will not send RIP messages but still receive them.

Routing loops: is due to the slow convergence of RIP and occurs when conflicting update information is received from different routers.
Maximum Hop Count: will set any network beyond a certain distance to be unreachable with the max hop count +1.
Split Horizon: enforces the rule that information cannot be sent back in the direction from which it was received.
Route Poisoning: sets down links to the unreachable value. It is followed by a poison reverse.
Hold-downs: timer that prevents conflicting rapid updates of the routing tables. Once a value is changed, the router will wait the hold-down timer prior accepting another change.
Triggered Updates: resets the hold-down timer if the timer expires, the router receives a processing task proportional to the number of links or another update is received indicating the network topology has changed. Creates a new routing table sent immediately to neighbour routers.

IGRP (Interior Gateway Routing Protocol): Cisco proprietary distance-vector routing protocol. Uses bandwidth, and delay as default metrics, and can also use reliability, load and Maximum Transmission Unit (MTU). IGRP can load-balance up to six unequal links. Routing information messages are sent every 90 sec by default.

(config)#**router igrp** *ASnumber*: enables RIP, but only shares information between the routers on the same autonomous system (AS).
(config-router)#**network** *network*: limits the propagation of the RIP messages to the *network*.
(config-router)#**variance** *multiplier*: number between 1 and 28 which controls the load balancing between the best and worst metric.
(config-router)#**traffic-share balanced**/**min**: share inversely proportional to metric or only routes that have minimum cost.

Other Routing Commands:
sh ip route: shows the routing tables. Also shows the administrative distance of each link, the hop count, the next hop and exit interface.
sh [**ip**] **protocols**: network layer address of each interface **or** (with **ip**) the routing protocols on the router and **timers** used.
debug ip rip/(**igrp events**/**transactions**): **rip** and **igrp transactions** send routing updates to the console. **igrp events** only sends a summary, including the destination and provenance, and the number of routers included in each message.
undebug all: turns off debugging. show debug will show what debug options are turned on.
ping *address*: verify connectivity with remote host.

Part VI – VLANs (Virtual LANs)

VLANs: logical grouping of network users and resources connected to administratively defined ports on a switch. The segmentation into VLAN creates smaller collision and broadcast domains and enhances security. Layer 3 switches or routers are needed to route packets between VLANs.

Switch Fabric: group of interconnected switches.

Dynamic vs static VLANs: Dynamic VLAN determine a host's VLAN assignment automatically from a MAC address table, protocols, or applications. VMPS (VLAN Management Policy Server) can be used to set up a database of MAC address-to-VLAN mappings. A static VLAN is one in which the administrator manually configured the port VLAN membership.

Access vs Trunk Links: Links that are part of one VLAN are access links. Devices attached to an access link are unaware of their VLAN membership. Trunk links can carry up to 1005 VLANs. A scheme is needed to identify what VLAN a frame belongs to (called frame tagging). ISL and IEEE 802.1q are two standards of frame tagging supported by Cisco switches.

Trunk Protocol: used with ISL or 802.1q to allow VLAN trunking.
ISL (Inter-Switch Link): proprietary to Cisco switches, and is used for FastEthernet or Gigabit Ethernet links only, on a switch port, router interface or a compatible server NIC. The server will then be able to be on multiple VLANs. The original frame is encapsulated with a 26-byte header and a 4-byte Frame Check Sequence (FCS) footer rather than modified. The ISL frames are up to 1522 bytes, which is over the Ethernet maximum of 1518.
802.1q: IEEE standard for frame tagging, required when using non-Cisco equipment. Inserts a field into the frame to identify the VLAN.

LANE (LAN Emulation): Used to communicate multiple VLANs over ATM.
802.10 (FDDI): used to send VLAN information over FDDI. Uses a SAID field in the frame header to identify the VLAN.

VTP (VLAN Trunk Protocol): Protocol created by Cisco to manage all the configured VLANs across a switched internetwork and to maintain consistency throughout the network. VTP allows an administrator to add, delete and rename VLANs which is then propagated to all the switches in the switch fabric. A VTP server must be created (default on switches). The other switches client or transparent (forward VTP information but do not accept updates) and must be on the same domain name to share information. Only the client does not store its configuration in NVRAM. The clients will update their information when a packet with a higher revision number is received. Updates are sent every 5 minutes or when a change occurs. Clients switches cannot make any changes, and transparent switches can make changes but the changes will remain local and not be broadcasted.

VTP Pruning: in order to reduce bandwidth, the VTP information will only be sent through trunk links which require the information. It is disabled by default on all switches. Once pruning is enabled on a VTP server, it is enabled for the whole domain. VLAN 1 is the administrative VLAN and is not eligible for pruning.

Router Switching Modes:

Mode	Description	Mode	Description
Process Switching	Frame copied on the router's process buffer. The router then performs a router performs a lookup on the Layer 3 address with the routing table, forwards the packet to the exit interface. The processor is very busy with routing.	Optimum Switching	Faster than fast switching because all processing is carried out on the interface processor including CRC.
Fast Switching	The first packet of a session is compared against the fast-switching cache then if no entry is found, packets are examined by the routing processor. Each interface processor calculates the CRC. Other packets from the same session will follow the same path.	Distributed Switching	Happens on Versatile Interface Processor (VIP) cards, which have a switching processor onboard, so very efficient. All required processing is done right on the VIP processor, which maintains a copy of the router's routing cache.
Autonomous Switching	Packets are compared to the autonomous switching cache on the interface processor, without interrupting the route processor.	Netflow Switching	Collects detailed data for use in conjunction with circuit accounting and application utilization information, but increases the overhead.
Silicon Switching	Only on 7000 Series routers equipped with a Silicon Switching Processor (SSP) Packets are compared to the silicon-switching cache on the silicon switching engine (SSE). Packets must still traverse the backplane of the router to get to the SSP and then back to the exit interface.	Cisco Express Forwarding (CEF)	Switching function designed for high-end backbone routers. It functions on Layer 3 and its biggest asset is the ability to remain stable in a large network. More efficient than both fast and optimum default switching paths. Doesn't rely on cached information, bur refers to two alternate resources: the Forward Information Base which is duplicated from the routing table, and the adjacency table, a Layer 2 MAC address table of connected routers.

Part VII – Network Management

Router Boot Sequence:
Router performs POST and verify that all components of the device are operational and present.
The bootstrap looks for and loads the Cisco IOS file. By default, the IOS is loaded from flash memory.
The IOS software looks for a valid configuration file stored in NVRAM (startup-config).
The startup-config file is loaded and ran, or the router will go in setup mode if no startup-config file is present.

Configuration Register: all Cisco routers have a 16-bit software register stored in NVRAM.

Bits	Description	Bits	Description
0-3	Boot Field: 00 – ROM Monitor, 01 – Boot Image from ROM 02-F – Use boot commands in NVRAM	11-12	Console line speed
6	Ignore NVRAM contents	13	Boot default ROM software if network boot fail
7	OEM Bit enabled	14	IP broadcasts do not have net numbers
8	Break disabled	15	Enable diagnostic messages and ignore NVRAM content
10	IP broadcast with all zeros		

The configuration register can be viewed with **sh version** and be changed with (config)#**config-register 0x***value* where *value* is a 4 digit hex number. If you need to interrupt the boot sequence by performing a break to change the configuration register and enter privilege dmode, use romon 1>**confreg 0x***value* followed by **reset** on a Cisco 2600 and **o/r 0x***value* followed by **i** on a Cisco 2500.

sh flash: displays the content and space available of Flash memory.
copy (**flash tftp**)/(**tftp flash**): used to backup or restore the IOS to or from a tftp server. Requires a default directory on the tftp server to work.
copy (**run**/**start tftp**)/(**tftp run**/**start**): used to backup or restore the running or startup config files. Each ! represent 1 UDP segment transmitted.
erase startup-config: erases the startup config file. The router will boot in setup mode the next time unless another startup config file is created.
config network: copy the config file from a TFTP server into RAM.
tftp server system *imagename*: used to configure a router as a tftp server that will be able to send the IOS to another router.

CDP (Cisco Discovery Protocol): protocol that gathers hardware and protocol information about neighbour devices for troubleshooting and documenting the network. The CDP **timer** specifies how often the CDP packets are sent, and the CDP **holdtime** is the duration the device will hold packets received from neighbour devices.

sh cdp [(**neighbor** [**detail**])]: displays the content of both timers or (neighbour) displays the information gathered about neighbour devices (hostname, interface packet is received on, capability, platform, interface from which the packet was broadcasted from and holdtime). The **detail** command will also display the IP address, protocols and IOS version of neighbouring devices (equivalent to **sh cdp entry ***)
(config)#**cdp timer**/**holdtime** *number*: used to change the value of either timer, which are defaulted to 60 and 180 seconds.
sh cdp traffic: outputs the number of packets sent and received and eventual errors with CDP.
sh cdp interface: shows the CDP status on router interface or switch port.
clear cdp table: clears the CDP table of information gathered about the neighbouring devices.
(config)#**no cdp run**: disable CDP for the whole router/switch.
(config-if)#[**no**] **cdp enable**: disable or enable CDP on a specific interface.

Telnet: once the VTY line password is set, you can telnet into a device. To switch from the remote connection to the local prompt, use the **Ctrl+Shift+6** key followed by **X**.
sh sessions: shows connections made to remote devices. The last session identified with a star can be returned to by pressing the **enter** key twice.
sh users: shows a list of users connected to your device. The * represent the session used to enter the command.
exit: to end the telnet session.
disconnect *number*: to close the telnet session *number* from the local console
clear line *number*: to terminate a connection from a remote host.

Resolving host names: it is possible to configure routers to store a host name table and use a DNS service.
(config)#**ip host** *name address*: adds an entry in the host table (use **no ip host** *name* to remove).
#**sh hosts**: displays the host table. The **perm** flag indicates a manual entry in the table, and the **temp** flag indicates an entry solved by DNS.

To configure a DNS server:
(config)#[**no**] **ip domain-lookup**: use no to disable. This is turned on by default.
(config)#**ip name-server** *address* **(Maximum of 6 DNS server addresses)**
(config#)[**ip domain-name** *name*]: Optional command that appends the domain name to the host name typed in.

Part VIII – IPX

General information:
IPX (Internetwork Packet Exchange) is a connectionless routable network protocol, such as UDP/IP and operates at layer 3 and 4 of the ISO model. IPX addresses are 80 bit long and are composed of a network (32 bits) and a node address (48 bits) in the following hexadecimal format nnnnnnnn.NNNN.NNNN.NNNN and the node address is typically the device's MAC address.
SPX (Sequenced Packet Exchange) provides connection-oriented transport for upper-layer protocols when needed.

SAP (Service Advertising Protocol) allows servers to advertise their own services and that of other known servers. Clients submit GNS (Get Nearest Server) request, which are answered by servers or routers based on their SAP tables, using a GNS reply. IF te information is unknown, no reply is sent. Routers do not re-broadcast GNS requests, but do update their SAP from all remote servers and send GNS replies to local clients. The SAP and RIP tables are sent every 60 seconds. A file server will be represented by service type 4.

RIP (Routing Information Protocol) distance-vector routing protocol that distributes the knowledge of IPX routes using hops and tick counts (1/18 second). An IPX address is represented by n.h.h.h (where n is the four-byte network address and h is the six-byte host address) is 80 bit long. The host address is often the host's MAC address, which enables IPX network to function without ARP or RARP protocols.

NLSP (NetWare Link Service Protocol): advanced link-state routing protocol intended to replace both SAP and RIP.

To enable IPX:
config t
ipx routing -> this also enables RIP and SAP but nothing will be broadcasted until the interfaces of the router are also configured.

To configure the interfaces:
int e0
ipx network *number* [**encapsulation** *type*][**secondary**]
no shutdown

where *type* takes one of the following:

Keyword	Type	Keyword	Type
Ethernet Interface		FDDI	
novell-ether (default)	Ethernet 802.3	**snap** (default)	FDDI snap
sap	Ethernet 802.2	**sap**	FDDI 802.2
arpa	Ethernet II (IPX Ethernet)	**novell-fddi**	FDDI raw
snap	Ethernet SNAP	Token Ring Interface	
Serial		**sap** (default)	Token Ring
hdlc (default)	HDLC	**snap**	Token Ring snap

Subinterfaces:
interface *type number.port* where *port* is between 0 and 4292967295 (and can be expressed in hexadecimal); or
int *typenumber.port* such as int e0.10

Note: when configuring a secondary frame type **or** subinterface, use a different network number

Other IPX commands:
show ipx route: shows the routing tables built from the RIP messages
show ipx servers: displays the router's SAP table. Clients will not see remote servers if their entry is not in the router's SAP.
show ipx traffic: displays a summary of the number and type of RIP and SAP packets received and transmitted by the **router**.
show ipx interface [*interface/***brief**]: displays status, **IPX address**, parameters of all/**one interface**(s) and RIP and SAP packets sent/received.
show protocols: indicates the routed protocols configured on the router. Also displays the **IPX address** of the interfaces.
debug/undebug ipx routing/sap activity/events: shows/hides IPX packets as running through the internetwork.
ping ipx *address*: pings the IPX address indicated by *address*.
ipx maximum-paths *number*: allows to perform load balancing on equal-cost paths to the same destination (*number* is between 1 (default) and 64). This information will be displayed by **show ipx route**.
ipx per-host-load-share: will force all packets sent to a destination or host to always go over the same line.

Part IX – Access Lists

Packets are compared to the access lists sequentially until a match is found. If no match is found, the packet is discarded. Access lists filter content going through the router, not the traffic originated by the router. You should place standard IP access lists as close to the destination as possible, whereas extended IP access lists should be as close from the source as possible. You can only assign two access lists per interface, one in each direction.

Access Lists	IP	IPX
Standard	Use source IP address	Use source and destination IPX address
Extended	Use source, destination IP address, protocol and port number	Use source, destination IPX address, Network layer protocol and socket number

To define a standard IP access list **(00<*number*<99)**:
config t
access-list *number* **deny**/**permit** *sourcehostname*/(*address matching- range)*/**any**/(**host** *address*)

The *number* will determine what protocol and type of access list it is. It is dependant on the IOS you are using.

When using *address matching-range*, the *matching-range* is defined by a set of wildcards corresponding to the number of addresses-1. The number of addresses are restricted to the power of two (1, 2, 4, 8, 16, 32, 64, 128, 256) thus the matching-range is restricted to (0, 1, 3, 7, 15, 31, 63, 127, 255). The address must also start at a multiple of the block size. For example, to allow 172.10.32.0 to 172.10.63.255, you would use the command:

access-list 10 **permit** 172.10.32.0 0.0.31.255. You would not be able to choose to permit from 172.10.35.0 to 172.10.66.255.

To define an extended IP access list **(100<*number*<199)**:
config t
access-list *number* **deny**/**dynamic**/**permit** *protocol* (*sourceaddress matching- range)*/**any**/(**host** *sourceaddress*)
[(*destaddress matching- range)*/**any**/(**host** *destaddress*)] [(**eq**/**neq**/**gt**/**lt** *port#*)/(**range** *port#start port#end*)] [**log**/**log-input**]

where *protocol* must be transport layer (tcp, udp or icmp) if you desire to filter out ports names. *port#* can also be a well known port name.

To define a standard IPX access list **(800<*number*<899)**:
config t
access-list *number* **deny**/**permit** *sourceaddress destaddress* (where –1 defines any.)

To define an extended IPX access list **(900<*number*<999)**:
config t
access-list *number* **deny**/**permit** *protocol sourceaddress sourcesocket destaddress destsocket*

To define an IPX SAP filter list **(1000<*number*<1099)**:
config t
access-list *number* **deny**/**permit** *sourceaddress servicetype*

To set an access list on an interface, once it has been defined:
int e0
ip access-group *number* **in/out**

To set an access list on a VTY line to control Telnet access:
line vty 0 4
access-class *number* **in/out**

To apply an IPX SAP filter to an interface, use:
ipx input-sap-filter/output-sap-filter *number* : stop SAP entries from being entered in the SAP table or from being propagated out.

Other access list commands:
show access-list [*number*]: displays all or a specific access list, but does not show what interface(s) it is applied to.
show ip access-list : shows only IP access lists on the router but doesn't indicate which interface (if any) they apply to.
show ipx access-list: shows only the access lists and SAP filters but doesn't indicate which interface (if any) they apply to.
show ip interface: shows which interfaces have access lists applied to.
show ipx interface [*interface/***brief**]: shows the IPX address of all or one interface, as well as its access list and inbound/outbound SAP filters.
show running-config: shows the access lists and what interfaces they are applied to.
clear access-list counters: resets the counters that keep the number of packets filtered at each line of an access-list.

Part X – WAN Protocols

Protocol	Meaning	Type	Layer	Characteristics
X25		Packet Switched	Data-link and Physical	ITU-T standard (International Telephone Union – Telecommunications Standardization Sector) Addresses expressed in decimal numbers in the following format:
Frame Relay		Packet Switched	Data-link and Physical	Connection-oriented and similar to X.25 with less overhead but does not provide error correction. More cost-effective than PPP. Uses Permanent Virtual Circuits (PVC) mostly but also Switched Virtual Circuits (SVC)
HLDC	High-Level Data Link Control	Dedicated Connection Bit Oriented	Data-link	peer-to-peer HDLC not intended to encapsulate multiple Network layer protocols across the same link, which prompted vendors to have their own **proprietary** HDLC protocol. No authentication is provided by HDLC. Default encapsulation of serial links, which have a default bandwidth of 1.54 Mbps (T1).
SDLC	Synchronous Data Link Control	Bit Oriented	Data-Link	Full-Duplex non peer-to-peer bit oriented serial protocol created by IBM.
ISDN	Integrated Services Digital Network	Circuit Switching	Physical, Data-link and Network, typically used with PPP.	Set of digital services that transmit voice and data over existing phone lines. The Basic Rate Interface (BRI) consists of two B channels at 64 kbps and one D channel at 16 kbps. PRI (Primary Rate Interface) T1 is 23 X 64kbps B channels and 1X 64 kbps D channel, and the PRI E1 is 30 X 64 kbps B channels and 1 X 64kbps D channel.
ATM	Asynchronous Transfer Mode			**53-byte cell** that allows fast hardware base switching. **LANE** (LAN Emulation) was created to hite ATM and look like 802.3 Ethernet.
PPP	Point-to-Point Protocol	Dedicated Connection	Data-link	Can be used to create point-to-point links between different vendors' equipment. Allows authentication and multilink connections and can be run over asynchronous (dial-up) and synchronous (ISDN) links. Created to replace SLIP (Serial Line Internet Protocol) which could only run IP at the Network Layer but was also a dedicated connection protocol. Stacker and Predictor compression methods are supported.
LAPB	Link Access Procedure, Balanced		Data-link	Connection-oriented, has tremendous amount of overhead for links that are error-prone. Defined by X.25 at the data-link layer

PPP:

Protocol Stack:

OSI Layer	PPP Protocol Stack	
3	Upper Layer Protocols such as IP, IPX, AppleTalk	
2 LLC	Network Control Protocol (NCP)	Specific to the Network Protocol used. Examples are IPCP (IP Control Protocol) and IPXCP (IPX Control Protocol)
2 MAC	Link Control Protocol (LCP)	Provides authentication with PAP (Password Authentication Protocol) or CHAP (Challenge Authentication Protocol), compression, error detection (with Quality and Magic Number) and multilink (splits the load for PPP over several parallel circuits.)
	High-Level Data Link Control Protocol (HDLC)	
1	Physical Layer (such as EIA/TIA-232, V.24, V.35, ISDN	

To enable PPP and authentication:
config t
hostname *hostname*
username *username* **password** *password*: *password* must be the same on both routers, and *username* corresponds to remote hostnam.e
int s0
encapsulation ppp
ppp authentication chap/**pap:** PAP is only performed upon the initial link estb and passwords are sent in clear. CHAP forces periodic checks.
sh int s0: verifies the PPP encapsulation.
debug ppp authentication: allows you to verify the PPP authentication configuration.

Frame Relay:

Uses the DLCI (Data Link Connection Identifier) which also identify the type of circuit (PVS or SVC) in order to allow two internet devices to communicate end-to-end through the frame relay cloud.
CIR (Committed Information Rate): Metric used when purchasing bandwidth, determining the guaranteed flow of traffic by the service provider. Traffic flow exceeding the CIR will not be guaranteed and retransmissions may occur.
DE (Discard Eligibility): When a Frame Relay router detects congestion on the network, the DE bit is turned on in. A congested switch will first discard these packets. A CIR of zero will have the DE bit always turned on.

FECN (Forward-Explicit Congestion Notification): When the Frame Relay network detects congestion in the cloud, this bit is turned on and the destination DTE (Data Terminal Equipment) is informed the path traversed is congested.
BECN (Backward-Explicit Congestion Notification): When the switch detects congestion in the network, the BECN bit is set and the packet sent to the source router, telling it to slow down the transmitting rate.

To enable Frame Relay. IARP (Inverse-ARP) or static frame-relay maps must also be defined for the Frame Relay devices to talk together::
config t
int s0
encapsulation frame-relay [**ietf**]: Cisco encapsulation is default, use **ietf** (Internet Engineering Task Force) to connect to non-Cisco devices.
frame-relay interface-dlci *number*: *number* is between 16-1007.
frame-relay lmi-type cisco/ansi/q933a: Local Management Interface. used only between router and service provider's switch. Provides information about the local or global significance of the DLCI value and the status of virtual circuits. **cisco** is default.

To create subinterfaces once the interface is configured:
int s0.*subintnumber* **multipoint/point-to-point**

To create maps which provide the DLCI to IP address conversion, if inverse-arp cannot be used, static maps must be defined:
no inverse-arp: inverse-arp, a different and dynamic method for converting DLCI to IP addresses. It must be turned off to enable frame relay maps.
frame-relay map ip *ip dlci* [**ietf/cisco**] [**broadcast**]: frame relay maps is the only way to mix both **cisco** and **ietf** encapsulation types.

Other commands:

sh frame-relay ip/lmi/map/pvc [*number*]/**route/traffic**: **sh frame pvc** and s**h running-config** will indicate DLCI number.
sh interface: displays LMI information and bandwidth as well as **sh frame lmi** and DLCI type but not the DLCI number.
debug frame-relay lmi

ISDN: Designed to run over existing telephone lines, can support both voice and data and sets up faster than conventional dial-up. Supports virtually every upper-layer protocol and you can choose PPP, HDLC, or LAPD (Link Access Procedure on the D Channel) as your encapsulation protocol.

TE1: Terminal Eqpt Type 1 understands ISDN standards and plug directly into the U or through a NT1 device in North-America.
TE2: devices that predate the ISDN standard and require a TA to connect to an NT1.
NT1: Network Termination 1 implements the ISDN physical layer specifications and connects users to the ISDN network.
NT2: is a provider's equipment such as a switch or PBX. Provides Data-Link (Q921) and Network Layer (Q931) implementations.
TA: converts TE2 wiring to TE1 wiring, and connects to an NT1.

Reference points		ISDN Standards defined by ITU	
R	between non-ISDN eqpt (TE2) and a TA (Terminal Adapter)	E Series	Using ISDN on existing phone networks
S	between the customer's router and an NT2		
T	between NT1 and NT2 devices (electrically same as S)	I Series	Concepts, aspects and services
U	between NT1 devices and line-termination eqpt in a carrier network (in N-A only)	Q Series	Switching and signalling

Interface Connection:
A router's U interface allows you to connect directly into the local loop (with the conventional two wires) and has a built-in NT1 connector. A S/T interface is a four-wire interface that needs a NT 1 converter from the two-wire ISDN specification and will connect to a TE1 device or to a TE2 device with a TA.

To enable ISDN:
config t
isdn switch-type basic-nil: contact your service provider to find out what switch to use. Can be configured globally or for each BRI.
int bri0
encap ppp (optional)
isdn spid1 086506610100 8650661: Service Profile Identifier similar to a phone number.
isdn spid2 086506610100 8650662: one for each channel.

Part XI – Catalyst 1900 Switch

The Catalyst 1900 Switch can be configured by a menu system, the Command Line Interface (CLI) or the Virtual Switch Manager (VSM) through a web browser once the IP address has been set. By pressing K at the first menu, you can access the CLI. The switch can table up to 1024 MAC addresses. The 1900 can use Store-and-Forward or FragmentFree (default) switching modes.

enable/disable: used to enter or exit the privileged mode

General commands entered in the **"#"** mode:
show version: displays basic IOS and switch information.
show ip: used to see the IP address settings on the switch, along with subnet, default gateway, domain name, and other parameters.
ping *address*: used to test connectivity from the switch. **telnet** or **traceroute** can only be used from a router.
delete nvram/vtp: erases the startup-config of a switch or VTP information. You cannot see the content of the startup-config on a switch, nor copy to or from it. Every changes made to the configuration is made to the NVRAM file immediately.
sh mac-address-table: displays the MAC address table.
clear mac-address-table dynamic/**permanent**/**restricted**: clears the address in the MAC address table that match the option chosen.
sh port system: displays information about switching type. Fragment-Free is the default switching mode.
sh vlan [*number*]: displays the VLAN information and port association about all VLANs or only the *number* VLAN.
sh vlan-membership: displays the VLAN information for all the interfaces.
sh trunk a/**b** [**allowed-vlans**/**joined-vlans**/**joining-vlans**/**prune-eligible**]: displays trunk information (port 26=A, 27=B).
copy tftp://*hostaddress*/*IOSfilename* **opcode**: used to update the IOS on the switch from a tftp server.
copy nvram tftp://*hostaddress*/*filename*: used to backup the startup-config file.
copy tftp://*hostaddress*/*filename* **nvram**: used to restore the startup-config file.
show cdp: displays cdp information.

config terminal: use to enter the terminal configuration

Commands entered in the **"(config)#"** mode:
hostname *name*: used to define a hostname that is locally significant only.
enable password level *number password*: used to set user and enable mode passwords (by setting *number* to either 1 or 15 respectively). *Password* must be between 4 and 8 characters and is not case sensitive.
en secret *password* : used to set the enable password using the encryption service. This will override the non-secure password if set.
ip (**address** *ipaddress subnetmask*)/(**default-gateway** *gatewayaddress*): used to set the IP address and subnet mask, or the gateway.
mac-address-table aging-time *time*: sets the aging time of dynamic addresses in .
mac-address-table permanent *address destinterface:* used to define permanent addresses.
mac-address-table restricted static *address destinterface sourceinterface*: used to define restricted addresses.
switching-mode fragment-free/**store-and-forward**: used to set the switching mode.
vlan *number* **name** *name*: defines VLANs. *number* is 1-1000. VLAN 1 is the default VLAN and all ports are associated to it. Maximum of 64 VLANs on a switch.
vtp server/**client**/(**domain** *name*)/(**password** *pw*)/(**pruning en**/**dis**)/**transparent**/**trap** : configures VLAN Trunk Protocol . Pruning is enabled on the whole domain if it is enabled on a server.
cdp advertise-v2/(**holdtime**/**timer** *seconds*): used to configure CDP (Cisco Discovery Protocol) information.

interface (**ethernet 0/***1-25*)/(**fastethernet 0/***26-27*) : the Ethernet interfaces are numbered 1-24, plus the serial port for AUI at the back, and the FastEthernet uplink ports are numbered 26-27. There is only one slot, slot 0.

Commands entered in the **"(config-if)#"** or **"(config-subif)#"** mode:
duplex auto/**full**/**full-flow-control**/**half** : used to change the duplex settings on a given port. **auto** is the default for 100BaseTX ports, and **half** is the default for 10BaseTX ports.
description *name*: used to define a description for the interface. *Name* must have underscores rather than spaces. **show run** and **show int 0/***n* will both show the descriptions set.
port secure max-mac-count *number*: will only allow *number* MAC addresses on the interface, and they will be permanent.
vlan-membership static/**dynamic** *number*: assigns a port to a VLAN. One VLAN per port unless trunking is used.
trunk auto/**desirable**/**nonegotiate**/**on**/**off**: used on the FastEthernet ports to enable trunking. All VLANs are allowed on the trunk by default.
no trunk-vlan *number*: to clear VLAN number from being trunked through this interface.
encapsulation isl *vlan_number*: in each subinterface of a trunk port, in order to support VLAN trunking.