Cisco™ CCENT : OSI and TCP/IP

OSI MODEL

Application : Responsible for identifying and establishing the availability of desired comm partner and verifying sufficient resources exist for comm. Ex: FTP, SMTP

Presentation : Responsible for presenting the data in standard formats. Some Presentation layer standards are JPEG, MPEG, MIDI, PICT, Quick Time, TIFF.

Session : Responsible for co-ordinating communication between systems/nodes. Some of the session layer protocols and interfaces: NFS, RPC, SQL, ASP, DNA SCP

Transport : Responsible for multiplexing upper-layer applications, session mgmt tearing down of virtual circuits, flow control and to maintain data integrity.

Network : Responsible for sending packets from the source network to the destination network using routing methods. Routers work at network layer.

Datalink : Consists of LLC sublayer and MAC sublayer. LLC handles error control, flow flow control, framing etc. MAC handles access to shared media such as ethernet.

Physical : Responsible for ultimate transmission of data over network communications media. Some of the standard interfaces at physical layer are EIA/TIA-232, V.24,V.35, HSSI

TCP/IP MODEL

Application : Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network. Ex: FTP, SMTP, Telnet

Transport : Provides communication session management between host computers. Ex: TCP, UDP

Internet : Performs routing of IP datagrams.
Ex: IP, ARP, ICMP

Physical : Controls the hardware devices and media that make up the network.

Some important port numbers

FTP : Port 20-21	Telnet : Port 23	DHCP : Ports 67 and 68	POP3 : Port 110
TFTP : Port 69	SMTP : Port 25	DNS : Port 53	HTTP : Port 80

Port numbers used by TCP/UDP

0-255 : Used for public applications
255-1023 : Assigned to companies
Above 1023 : Used by upper layers to set up sessions with other hosts and by TCP to use as source and destination addresses.

Cisco™ CCENT : IOS

Internal memory components of a cisco router

ROM : Memory containing micro-code for basic functions to start and maintain the router.
RAM/DRAM : Stores the running configuration, routing tables, and packet buffers.
NVRAM : Memory that does not lose information when power is lost. Stores the system's configuration file and the configuration register.
Flash Memory : Stores the compressed IOS image.

Router Default Boot Sequence for Cisco IOS

1. NVRAM
2. Flash (sequential)
3. TFTP server
4. ROM

The router first looks at Startup Config file in NV RAM, if not available, it falls back to Flash, then to TFTP and then to ROM.

Router boot configuration commands

boot system ROM : boots from system ROM
boot system flash <IOS file name> : boots IOS from flash memory
boot system tftp <IOS file name>
<tftp_addr> : boots IOS from a tftp server

Router Cursor Commands

<ctrl> A: Move to the beginning of the command line
<ctrl> E: Move to the end of the command line
<ctrl> F: Move forward one character, same as using "Right Arrow"
<ctrl> B: Move backward one character, same as using "Left Arrow".
<ctrl> P: Repeat Previous command, same as using "Up Arrow"
<ctrl> N: Repeat Next (more recent) command, same as using "Down Arrow"
<esc> B: Moves to beginning of previous word.
<esc> F: Moves to beginning of next word.
<ctrl>R: Creates new command prompt, followed by all the characters typed at the last one.

Configuration Register Command

Router(config)# config-register *0x10x* *(where that last x is 0-F in hex)*, when the last x is: **0** = boot into ROM Monitor mode; **1** = boot the ROM IOS; **2 - 15** = look in startup-config file in NVRAM.

Cisco router configurable locations

Console port, Virtual Terminals (vty), Auxiliary port, TFTP server and Network management station

Router modes of operation include

Mode	Prompt
user exec	Router>
Privileged	Router #
global config	Router(config)#
Interface config	Router(config-if)#

Router passwords

Enable password
Console password
Enable Secret
Virtual terminal password (vty)
Auxiliary password

Three ways router learns to forward packets

1. **Static routes** : Configured by the administrator manually. Syntax : ip route <ip-addr><mask-addr><ip-addr>
   Ex: R1(config)#ip route 192.168.200.0 255.255.255.0 192.168.1.2
2. **Default routes** : This is used when a route is not known or is infeasible. Syntax : ip route 0.0.0.0 0.0.0.0 <ip-addr>
   Ex: R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2
3. **Dynamic routes** : In dynamic routing, the routing tables are automatically updated.
   Dynamic routing uses broadcasts and multicasts to communicate with other routers.

More info

To enable the Cisco IOS to forward packets destined for obscure subnets of directly connected networks onto the best route, use "ip classless" command.

By default, Cisco routers support 5 simultaneous telnet sessions. This number can be configured using IOS commands.

Cisco™ CCENT : Password Recovery

Procedure 1

Complete these steps in order to recover your password:

1. Attach a terminal or PC with terminal emulation to the console port of the router and set terminal settings to 9600 baud rate, No parity, 8 data bits, 1 stop bit, No flow control.
   The configuration register is usually set to 0x2102 or 0x102. If you can no longer access the router you can safely assume that your configuration register is set to *0x2102*.
2. Use the power switch in order to turn off the router, and then turn the router back on.
3. Press **Break** on the terminal keyboard within 60 seconds of power up in order to put the router into ROMmon.
4. Type **confreg 0x2142** at the rommon 1> prompt in order to boot from Flash. This step bypasses the startup configuration where the passwords are stored.
5. Type **reset** at the rommon 2> prompt.
   The router reboots, but ignores the saved configuration.
6. Type **no** after each setup question, or press **Ctrl-C** in order to skip the initial setup procedure.
7. Type **enable** at the Router> prompt.
   You are in enable mode and should see the Router# prompt.
8. Type **configure memory** or **copy startup-config running-config** in order to copy the nonvolatile RAM (NVRAM) into memory.
9. Type **configure terminal**.
   The router(config)# prompt appears.
10. Type **enable secret <***password***>** in order to change the **enable secret** password.
    For example:
    router(config)**#enable secret** *cisco*
11. Issue the **no shutdown** command on every interface that you use.
12. Type **write memory** or **copy running-config startup-config** in order to commit the changes.

Procedure 2

Complete these steps in order to recover your password:

1. Shut down the router.
2. Remove the compact flash that is at the back of the router.
3. Power on the router.
4. Once the Rommon1> prompt appears, enter this command:
   confreg 0x2142
5. Insert the compact flash.
6. Type **reset**.
7. When you are prompted to *enter the initial configuration*, type **No**, and press **Enter**.
8. At the Router> prompt, type **enable**.
9. At the Router# prompt, enter the **configure memory** command, and press **Enter** in order to copy the startup configuration to the running configuration.
10. Use the **config t** command in order to enter global configuration mode.
11. Use this command in order to create a new user name and password:
    router(config)**#username cisco password cisco**
12. Use this command in order to change the boot statement:
    config-register 0x2102
13. Use this commnd in order to save the configuration:
    write memory

Reload the router, and then use the new user name and password to log in to the router.

Note : The given procedures are generic in nature, and for exact sequence of steps, please refer to product manual.

Cisco™ CCENT : IPv4 Addressing

Converting Binary to Decimal

Binary is a base 2 system with only two numbers 0 or 1.
The weightage of binary digits from right most bit position to the left most bit position is given below.

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Example :

Convert 10011101 into a decimal value.
There are eight bits in the binary number. The decimal value for each bit position is given below:

128	64	32	16	8	4	2	1	« Decimal equivalent of the binary position
1	0	0	1	1	1	0	1	« Given binary number

To convert, you simply take a value from the top row wherever there is a 1 below, and then add the values together.

i.e, **$1*2_7 + 0*2_6 + 0*2_5 + 1*2_4 + 1*2_3 + 1*2_2 + 0*2_1 + 1*2_0$**

= 128 + 0 + 0 + 16 + 8 + 4 + 0 + 1

= 157 (decimal value)

Converting Decimal to Binary

Decimal is a Base 10 system with 10 possible values (0 to 9)

To convert decimal to binary, simply divide the decimal value by 2 and then write down the remainder, repeat this process until you cannot divide by 2 anymore.

For example, take the decimal value **157**:

157 ÷ 2 = 78 with a remainder of 1
39 ÷ 2 = 19 with a remainder of 1
9 ÷ 2 = 4 with a remainder of 1
2 ÷ 2 = 1 with a remainder of 0

78 ÷ 2 = 39 with a remainder of 0
19 ÷ 2 = 9 with a remainder of 1
4 ÷ 2 = 2 with a remainder of 0
1 ÷ 2 = 0 with a remainder of 1

To convert, write this remainder first---------->

Next write down the value of the remainders from bottom to top (in other words write down the bottom remainder first and work your way up the list) which gives:

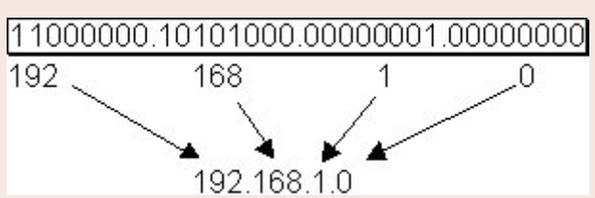
10011101 = 157

Cisco™ CCENT : IPv4 Addressing

IP Address Intro

1. An IP address (32 bit number, 4 bytes) consists of four octets seperated by dots.

The octet is a binary number of eight digits, which equals the decimal numbers from 0 to 255.



2. The internet protocol defines the special network address **127.0.0.1** as a local loopback address.

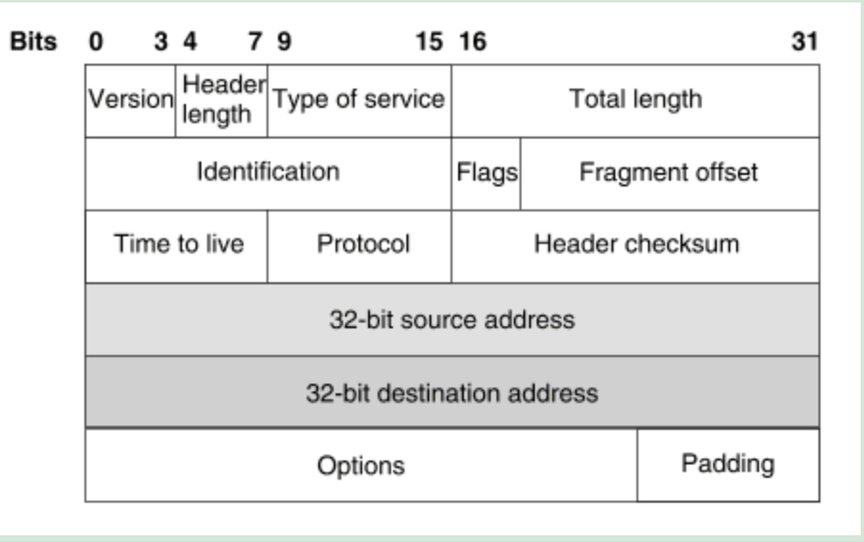
IP Address Classes (Public IP range)

Class	Format	Leading-bit-pattern	Network-addr-range	Max-netw	Max-hosts
A	N.H.H.H	0	0-126	127	16,777,214
B	N.N.H.H	10	128-191	16,384	65,534
C	N.N.N.H	110	192 -223	2,097,152	254

Class D addresses are used for multicasting, they begin with “1110” and the addr range is 224-239.
Class E addresses are reserved addresses that begin with “11110” and the range is 240-254.

Private addr range : **Class A** : 10.0.0.0 to 10.255.255.255, **Class B** : 172.16.0.0 to 172.31.255.255, **Class C** : 192.168.0.0 to 192.168.255.255

IPV4 Header



Subnet Mask and CIDR notation

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address.

Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s.

Default Subnet Masks

Class A : 255.0.0.0, Class B : 255.255.0.0, Class C : 255.255.255.0

CIDR Notation : Classless Inter Domain Routing (CIDR) is a method for assigning IP addresses without using the standard IP address classes like Class A, Class B or Class C.

In CIDR notation, an IP address is represented as A.B.C.D /n, where "/n" is called the IP prefix or network prefix. The IP prefix identifies the number of significant bits used to identify a network.

Ex: 216.3.128.12, with subnet mask of 255.255.255.128 may be written as 216.3.128.12/25 using CIDR Notation.

Cisco™ CCENT : Subnetting

Requirement for IPv4 Subnetting

1. Efficient use of available IP address space
2. Network traffic isolation
3. Improved security
4. Limiting broadcast messages

Subnetting Scenarios

The subnetting scenarios may broadly be divided in to two categories:
1. Optimize for a given number of hosts
2. Optimize for a given number of subnets

Finally, determine the host address range for each available subnet.

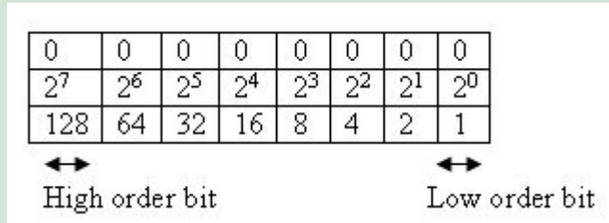
Subnetting Scenario Question 1

You want X number of subnets, what is the subnet mask ? (Assume we need 10 subnets, i.e, X=10)

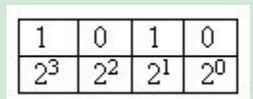
Tip : Convert X to binary, determine how many low order bits need to make the number, that many bits is number of high order bits that make up your subnet mask, convert high order bits to decimal value.

Solution :

Consider the Class C address – N.N.N.H where N is the Network portion and H is the host portion. Host Portion is as shown ----->



Step 1: Convert 10 to binary. Binary equivalent of 10 is as shown --------->

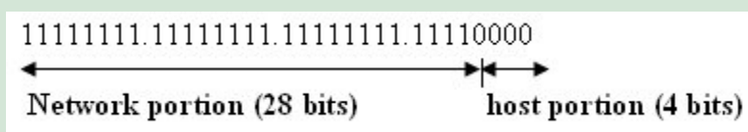


Step 2: Number of low order bits required to make the number is 4 (from the figure shown above)

Step 3: Therefore 4 high-order bits make up the subnet mask, i.e, 128, 64, 32, 16

Add 4 high order bits to create subnet mask i.e. 128+64+32+16=240 (11110000). The subnet mask is **255.255.255.255.240**

255.255.255.240 is represented as -------->



Cisco™ CCENT : Subnetting

Subnetting Scenario Question 2

How many subnet bits are required for X number of hosts ? (Assume X value to be 5 in this case)

Tip : Convert X (for the subnets) to binary, determine the number of bits needed for the host portion, additionally determine the subnet mask from the remaining bits, using formula 2^n, find the relevant number of subnets in this scenario.

Solution :

Step 1: Consider the Class C address N.N.N.H, where H is the host portion whose binary and decimal representation is as shown ---->

0	0	0	0	0	0	0	0
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Convert 5 to binary. Binary equivalent of 5 is as shown --------->

0	0	0	0	0	1	0	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Step 2: As shown in the figure above, the number of bits needed for the host portion are 3. Therefore, $2^{bits}-2=2_3-2=6$ (6>5)

3 bits are required for the host portion for 5 hosts.

Step 3 (Additional): To know the subnet mask , add the decimal value of the remaining 5 bits i.e, (128+64+32+16+8) = 248

Subnet Mask is 255.255.255.248 (11111111.11111111.11111111.11111000)

Number of subnet bits: 29, here 5 bits are used from the host portion of our subnet mask

Therefore number of subnets required is (2_n), where 'n' is the number of bits being used from the host portion of our subnet mask i.e. 5

Therefore, $2_5=32$ is the number of subnets

Cisco™ CCENT : Subnetting

Subnetting Scenario Question 3

Determine the range of valid IP Addresses for an X subnet mask ? (Assume X value to be 240 in this case)

Tip : Convert X to binary and determine the decimal value of lowest high order bit, start the range of addresses at that value, and increment the range by that value.

.

Solution :

Step 1: Convert 240 to binary. Binary equivalent of 240 is as shown --------->

1	1	1	1	0	0	0	0
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Step 2: The decimal value of lowest high order bit is 16 (2^4) as seen from the figure above. Therefore, this number becomes the increment value to determine the IP address ranges.

Subnet Mask: 255.255.255.240
Subnet Bits: 28 Host Bits: 4
Number of Subnets: 16 Hosts per Subnet: 14

The range of addresses for the given mask is as shown ------>

Network Addresses	Host Addresses IP Range	Broadcast Address
.0	.1-.14	.15
.16	.17-.30	.31
.32	.33-.46	.47
.48	.49-.62	.63
.64	.65-.78	.79
.80	.81-.94	.95
.96	.97-.110	.111
.112	.113-.126	.127
.128	.129-.142	.143
.144	.145-.158	.159
.160	.161-.174	.175
.176	.177-.190	.191
.192	.193-.206	.207
.208	.209-.222	.223
.224	.225-.238	.239
.240	.241-.254	.255

Note: All zeros and all ones host addresses cannot be used.

Cisco™ CCENT : Routing Protocols

Routing Protocols

Routing protocols job is to maintain routing tables and route packets appropriately.

Examples of routing are RIP, IGRP, EIGRP, OSPF.

Routed Protocols

Routed protocols are used to transport user traffic from source node to destination node.
Examples of routed protocols are IP, IPX and AppleTalk.

Classful Routing Protocols

Classful routing protocols do not exchange subnet information during routing information exchanges.
The summarization is always done automatically at major network boundaries.
Ex: RIP v1, IGRP

Classless Routing Protocols

In classless routing protocols, subnet information is exchanged during routing updates.
This results in more efficient utilization of IP addresses. The summarization in classless networks is manually controlled. Ex: RIP v2, EIGRP, OSPF, BGP v4, and IS-IS

Types of Routing Protocols

Distance Vector: Distance vector routing determines the direction and distance to any link in the internetwork. Smaller the metric, better the path. Distance vector routing is useful for smaller networks. Ex: RIP and IGRP.

Link State: Also known as SPF algorithms, SPF generates the exact topology of the entire network for route computation by listening to the first hand information. Bandwidth and delay are the most widely used metrics. Ex: OSPF and NLSP.

Balanced Hybrid: Balanced Hybrid combines some aspects of Link State and Distance Vector routing protocols. It uses distance vectors with more accurate metrics to determine the best paths to destination networks. Ex: EIGRP

Default Administrative distances

Directly Connected Interface------> 0
Static Route------> 1
Internal EIGRP------> 90
IGRP------> 100
OSPF------> 110
RIP------> 120
IS-IS------> 115
Unknown 255
External BGP----------> 20
Internal BGP----------> 200
An administrative distance of 0 represents highest trustworthiness of the route.
An administrative distance of 255 represents the lowest trustworthiness of the route.

ARP

Address Resolution Protocol (ARP) is used to resolve a hosts IP address to its physical address (such as MAC address), to allow communication on a multi-access medium such as ethernet.

Reverse ARP (RARP) is used to obtain an IP address from physical address (such as MAC). RARP broadcast may be used to obtain IP address to boot by diskless workstations over a network.

Cisco™ CCENT : NAT

Static NAT

Maps an unregistered IP address to registered IP (globally unique) addresses on one-to-one basis.

The command, **ip nat inside source static <local ip> <global ip>** configures address translation for static NAT.

Dynamic NAT

Maps an unregistered IP address to a registered (globally unique) IP address from a group of registered (globally unique) IP addresses.

The command, **ip nat inside source list <access-list-number> pool <name>** is used to map the access-list to the IP NAT pool during the configuration of Dynamic NAT.

Overloading

A special case of dynamic NAT that maps multiple unregistered IP addresses to a single registered (globally unique) IP address by using different port numbers.

Dynamic NAT with overloading is also known also as PAT (Port Address Translation).

Overlapping

This occurs when your internal IP addresses belong to global IP address range that belong to another network.

Defining an IP NAT Pool

1. Defining an IP NAT pool for the inside network using the command:
ip nat pool <pool-name> <start-ip> <end-ip> {netmask <net-mask> | prefix-length <prefix-length>} [type-rotary] ***Ex: ip nat pool pool1 200.200.200.3 200.200.200.4 netmask 255.255.255.0***

Note that type-rotary is optional command. It indicates that the IP address range in the address pool identifies hosts among which TCP load is distributed.

2. Mapping the access-list to the IP NAT pool by using the command:
ip nat inside source list <access-list-number> pool <pool-name> ***Ex: ip nat inside source list 1 pool pool1***

Address Classification

Inside Local : An actual address assigned to an inside host

Inside Global : An inside address seen from the outside

Outside Global : An actual address assigned to an outside host

Outside Local : An outside address seen from the inside

NAT Pool : A pool of IP addresses to be used as inside global or outside local addresses in translations

Configuring NAT

When configuring NAT, NAT should be enabled on at least one inside and one outside interface.

1. The command for enabling NAT on inside interface is:
R1(config-if)#ip nat inside

2. The command for enabling NAT on the outside interface is:

R1(config-if)#ip nat outside

Remember to enter into appropriate configuration modes before entering the commands.

Usually, the inside NAT will be configured on an Ethernet interface, whereas the outside NAT is configured on a serial interface.

Cisco™ CCENT : Configuration Commands

	A. Setting Passwords	
Sl. No.	**Task**	**Commands**
1	Configure router console password as "ciscocs"	R1(config)#line console 0 R1(config-line)#login R1(config-line)#password ciscocs
2	Configure router vty password as "ciscovty"	R1(config)#line vty 0 4 R1(config-line)#login R1(config-line)#password ciscovty
3	Configure router auxiliary password as "ciscoaux"	R1(config)#line aux 0 R1(config-line)#login R1(config-line)#password ciscoaux
4	Set the encrypted enable password as "cisco"	R1(config)#enable secret cisco
5	Set the unencrypted enable password as "ccna"	R1(config)#enable password ccna
	B. Router Copy Commands	
6	Copy the running-configuration to startup-configuration (DRAM to NVRAM)	R1#copy running-config startup-config (copy run start)
7	Copy the startup-configuration to running-configuration (NVRAM to DRAM)	R1#copy startup-config running-config (copy start run)
8	Copy the startup-configuration to a TFTP server	R1#copy startup-config tftp (copy start tftp)
9	Copy the running-configuration to a TFTP server	R1#copy running-config tftp (copy run tftp)
10	Save a backup of the IOS to a TFTP server	R1#copy flash tftp
11	Upgrade the IOS from a TFTP server	R1#copy tftp flash
	C. Routing Commands	
12	Enable RIP version1 on all 192.168.x.x interfaces	R1(config)#router rip R1(config-router)#network 192.168.0.0
13	Enable RIP version 2	R1(config)#router rip R1(config-router)#version 2

Cisco™ CCENT : Show Commands

Router Show commands		
Sl. No.	**Command**	**Explanation**
1.	show access-list	Displays all accesslists from all protocols present in a specified router.
2.	show banner	Displays the banner set on the router.
3.	show cdp	Shows the status of CDP such as holdtime value,no.of packets for every 60sec.
4.	show cdp interface	It tells the CDP configuration on an interface-by-interface basis.
5.	show cdp neighbor|detail	Displays info on directly connected neighbors.
6.	show cdp traffic	Displays the CDP traffic info.
7.	show clock	Displays the clock (time, date).
8.	show flash	Used to view all IOS images and file stored in flash(Default location of IOS images is in flash).
9.	show history	Shows the previously executed commands.IOS device stores the last ten commands that are executed.
10.	show hosts	Displays the host table.
11.	show interfaces	To view interfaces,status,and statistics for an interface.If u don't lists a specific interface,all of the interfaces on the router are listed.
12.	show ip interfaces	Displays status and global parameters associated with the interfaces on the router.
13.	show ip interface brief	Displays the interface operational status and IP addresses for all router interfaces.
14.	show ip nat statistics	Displays NAT statistics.
15.	show ip nat translations	Displays the NAT translations.
16.	show ip route	Displays the IP routing table.
17.	show protocols	Displays the routing protocols that have been configured and running on a specified router.
18.	show running-config	Shows the current config stored in RAM.
19.	show sessions	Shows the telnet sessions that are currently suspended.
20.	show startup-config	Shows the configuration stored in NVRAM.
21.	show version	Display version information for the hardware and firmware.
22.	show arp	Displays entries in the ARP table.
23.	show ip protocols	Displays parameters and current state of the active routing protocol process.
24.	show users	Displays users connected to the router.

Cisco™ CCENT : Show Commands

Switch Show commands		
Sl. No.	**Command**	**Explanation**
1.	show banner	Displays the banner.
2.	show flash	Displays the file contents of the flash.
3.	show history	Displays the last 10 commands entered.
4.	show interfaces	To view interfaces,status,and statistics for an interface.
5.	show interfaces vlan 1	Displays the VLAN status and the IP address of VLAN 1.
6.	show ip interface brief	Verifies the IP configuration.
7.	show running-config	Displays the config held in DRAM.
8.	show startup-config	Displays the NVRAM config.
9.	show users	Displays the users currently logged on.
10.	show version	Display IOS version information for the hardware and firmware.
11.	show vlan	Displays vlan information.
12.	show vlan-membership	Displays vlan membership information.
13.	show mac-address-table	Displays mac-address-table information.
14.	show vtp status	Displays vtp status information such as vtp mode, vtp domain etc.