

## **Unit 4 SWITCH**

### **SEVEN MARKS :**

4) Give the different CLI modes and its significance with CISCO Switches

ANS : In Cisco switches, the CLI (Command Line Interface) operates through different modes, each serving a specific purpose:

1. \*User EXEC mode (User Mode):\* Identified by the ">" symbol, this mode allows basic monitoring commands but limits configuration changes. It's the initial mode upon logging in.
2. \*Privileged EXEC mode (Privileged Mode):\* Identified by the "#" symbol, it grants access to all commands, including configuration, and allows for more in-depth changes to the system.
3. \*Global Configuration mode:\* Accessed from Privileged EXEC mode by using the "configure terminal" command. This mode enables configuration changes for the entire system, including interfaces, protocols, and other global settings.
4. \*Interface Configuration mode:\* Entered from Global Configuration mode using the "interface [interface type and number]" command. This mode permits configuration changes for a specific interface, like Ethernet or VLAN interfaces.

Understanding and navigating these CLI modes are crucial as they allow users to progressively access and modify different levels of switch configurations, ensuring proper management and control over the device.

---

5).What are the different levels of passwords & its significances in a CISCO Switches?

ANS : In Cisco switches, passwords are used to control access to different privilege levels. There are primarily two significant password levels:

1. \*User EXEC Mode password:\* This password restricts access to the User EXEC mode, allowing users to view but not change the switch's configuration. It provides basic monitoring capabilities.

2. \*Privileged EXEC Mode password:\* This password restricts access to the Privileged EXEC mode, which allows for complete control over the switch, including configuration changes.

Having different passwords for these levels helps in enforcing security measures, ensuring that only authorized individuals can access and modify the switch's configurations. It's a vital aspect of network security, especially in preventing unauthorized changes that could disrupt network operations or compromise sensitive information.

---

6).Give the procedure to assign passwords to a CISCO Switch

ANS : You can set

- ☐ The user mode passwords (Login pwd)
- ☐ The privileged mode passwords

used to verify authorization of the switch, including  
accessing any line and the console.

used to allow access to the switch so that configuration  
can be viewed as well as changed

Passwords cannot be less than four characters or more  
than eight.

They are not case sensitive.

>

>enable

#config t

(config)#enable password ?

level Set exec level password

(config)#enable password level ?

<1-15> Level number

(config)#enable password level 1 srinivas

(config)#enable password level 1 srinivas

>

>enable

#config t

(config)#enable password ?

level Set exec level password

(config)#enable password level ?

<1-15> Level number

(config)#enable password level 15 mcasu

config)#

(config)#enable password level 15 mcasu

1 user(s) now active on Management Console.

User Interface Menu

[M] Menus

[K] Command Line

[I] IP Configuration

Enter Selection:K

Enter password:\*\*\*\*\*

CLI session with the switch is open. To end the CLI session, enter [Exit].

>enable

Enter password:\*\*\*\*

#

enable secret password is a more secure password and supersedes the enable password

(config)#enable secret bhatsir

use the command show running-config (show run) to see the current configuration on the switch

#sh run

Building configuration...

Current configuration:

Enable secret 5\$1\$FMFQ\$wFVYVLYn2aXscfB3J95.w.

enable password level 1 "SRINIVAS"

Enable password level 15 "MCASU"

---

8) Give the procedure to assign hostname & description for an interface on a CISCO Switch

ANS : The hostname on a switch, as well as on a router, is only locally significant. This means that it doesn't have any function on the network or name resolution whatsoever. However, it is helpful to set a hostname on a switch so that you can identify the switch when connecting to it. A good rule of thumb is to name the switch after the location it is serving. The 1900 switch command to set the hostname is exactly like any router: you use the hostname command. Remember, it is one word. The switch out-put below shows the console screen. Press K to go into user mode, enter the password, use the enable command, and enter the enable secret password. From global configuration mode, type the command hostname hostname. 1 user(s) now active on Management Console.

```
>en
```

```
Enter password:***
```

```
#config t
```

```
Enter configuration commands, one per line.
```

```
CNTL/Z
```

```
(config)#hostname Todd1900EN
```

```
Todd1900EN(config)#
```

You can administratively set a name for each interface on the 1900 switch. Like the hostname, the descriptions are only locally significant. For the 1900 series switch, use the description command. You cannot use spaces with the description command, but you can use underscores if you need to.

#### Setting Descriptions

To set the descriptions, you need to be in interface configuration mode. From interface configuration mode, use the description command to describe each interface. You can make the descriptions more than one word, but you can't use spaces. You'll have to use the underscore as shown below:

```
Todd1900EN#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z
```

```
Todd1900EN(config)#int e0/1
```

```
Todd1900EN(config-if)#description Finance_VLAN
```

```
Todd1900EN(config-if)#int f0/26
```

```
Todd1900EN(config-if)#description trunk_to_Building_4
```

```
Todd1900EN(config-if)#
```

---

9)What are the different Duplex settings for a switch interface? Explain

Configuring the Port Duplex

ANS : The 1900 switch has only 12 or 24 10BaseT ports and comes with one or two FastEthernet

ports. You can only set the duplex on the 1900 switch, as the ports are all fixed speeds.

Use the duplex command in interface configuration.

In the switch output below, notice the options available on the Fast-Ethernet ports.

Todd1900EN(config)#int f0/26

Todd1900EN(config-if)#duplex ?

Auto            Enable auto duplex configuration

Full            Force full duplex operation

full-flow-control      Force full duplex with flow control

Half            Force half duplex operation

---

11)What is the significance of Permanent mac address in mac address table? How to set this add?

ANS : Administrators can specifically assign permanent addresses to a switch port. These addresses are never aged out. You can do this to provide security to a port, which means that unless you specifically configure a hardware address to a switch port, it won't work.

Administrators can also create static entries in the switch; these entries actually create a path for a source hardware address. This can be really restrictive, and you need to be careful when setting static entries because you can basically shut your switch down if you do not plan the configuration carefully.

You can configure a permanent MAC address to a switch

port by using command

mac-address-table permanent [mac-address]

[interface].

After you choose the mac-address-table permanent

command, add the hardware address and the interface it is

associated with.

Todd1900EN(config)#mac-address-table permanent ?

48 bit hardware address

Todd1900EN(config)#mac-address-table permanent 00A0.2448.60A5 e0/4

This will restrict the interface e0/4 to only accept frames from 00A0.2448.60A5 source hardware address.

```
Todd1900EN#sh mac-address-table
```

Number of permanent addresses : 1

Number of restricted static addresses : 0

Number of dynamic addresses : 3

Address	Dest Int	Type	Source Int
00A0.2448.60A5	Ethernet 0/4	Permanent	All
0000.8147.4E11	Ethernet 0/5	Dynamic	All
0000.8610.C16F	Ethernet 0/1	Dynamic	All
00A0.246E.0FA8	Ethernet 0/2	Dynamic	All

---

14) Give the procedure to create 4 vlans and assign port membership to each on a Switch

ANS : You can configure each port to be in a VLAN by using the vlan-membership command. You

can only configure VLANs one port at a time. There is no command to assign more than one port to a VLAN at a time with the 1900 switch.

Remember that you can configure either static memberships or dynamic memberships on a port. This book and the CCNA exam objectives only cover the static VLAN memberships.

In the following example, I configure interface 2 to VLAN 2, interface 4 to VLAN 3, and interface 5 to VLAN 4.

```
1900EN#config t
```

Enter configuration commands, one per line.

End with CNTL/Z

```
1900EN(config)#int e0/2
```

```
1900EN(config-if)#vlan-membership ?
```

```
1900EN(config-if)#vlan-membership static ?
```

```
<1-1005> ISL VLAN index
```

```
1900EN(config-if)#vlan-membership static 2
```

```
1900EN(config-if)#exit
```

```
1900EN(config)#int e0/4
```

```
1900EN (config-if)#vlan-membership static 3
```

```
1900EN(config-if)#exit
```

```
1900EN(config) #int e0/5
```

```
1900EN(config-if)#vlan-membership static 4
```

```
1900EN(config-if)#exit
```

```
1900EN(config)#exit
```

Now, type show vlan again to see the ports assigned to each VLAN.

```
1900EN#sh vlan
```

```
VLAN Name Status Ports
```

```
-----
```

```
1 Default Enabled 1, 3, 6-12, AUI, A, B
```

```
2 Sales Enabled 2
```

```
3 marketing Enabled 4
```

```
dynamic Set VLAN membership type as Dynamic
```

```
Static Set VLAN membership type as Static
```

```
4 Mis Enabled 5
```

```
1002 fddi-default Suspended
```

```
1003
```

```
token-ringdefau Suspended
```

```
1004 fddinet-default Suspended
```

```
1005 trnet-default Suspended
```

```
-----
```

```
[ouput cut]
```

You could also just type show vlan # to gather information about only one VLAN at a time.

```
1900EN#sh vlan 2
```

```
VLAN Name Status Ports
```

```
-----
```

```
2 sales Enabled 2
```

```
-----
```

```
VLAN Type SAID MTU Parent RingNo BridgeNo Stp
```

Trans1 Trans2

-----  
2 Ethernet 100002 1500 0 1 1 Unkn 0 0

1900EN#

Another command you can use to see the ports assigned to a VLAN is show vlanmembership. Notice that this command shows each port on the switch, which VLAN the port is a member of, and the membership type (static or dynamic).

1900A#sh vlan- membership Port VLAN Membership

1 1 Static

2 2 Static

3 1 Static

4 4 Static

5 5 Static

6 1 Static

7 1 Static

8 1 Static

9 1 Static

10 1 Static

11 1 Static

12 1 Static

AUI 1 Static

A 1 Static

B 1 Static

---

15) Demonstrate an ISL routing on a single router interface to implement inter VLAN routing

ANS : To support ISL routing on one FastEthernet interface, the router's interface is divided into

logical interfaces, one for each VLAN. These are called sub-interfaces. Since we have four VLANs, we need four subinterfaces. Each one of the VLANs is a separate subnet, so here is the addressing I want to use:

Each of the hosts in their VLAN must use the same subnet addressing. To configure the router-on-a-stick for inter-VLAN routing, you need to complete three steps:



- ❑ Enable ISL trunking on the switch port the router connects to
- ❑ Enable ISL encapsulation on the router's sub interface.
- ❑ Assign an IP address to the sub interface and other logically addressing if applicable (IPX, for example).

To create a sub interface from global configuration mode, choose the Fast Ethernet interface, a period, and then a number. You will now be in the (config-subif) prompt for the interface. To configure ISL routing on a sub interface, use the encapsulation isl [vlannumber] command. You can then assign an IP address, IPX address, AppleTalk address, etc., to the sub interface. This is a unique subnet and all the hosts on that VLAN should be in that same subnet. It is not required but is highly recommended. Here is how to configure the 2621 router to support ISL routing with our four VLANs. First, I'll configure a sub interface with the same number as the VLAN I want to route. This is locally significant only, which means it doesn't matter at all what the sub interface numbers are on the network. Notice that you need to set the encapsulation next, or you will receive an error when trying to set the sub interface's IP address. VLAN 1 is in the 172.16.10.0 network. I need to assign a sub interface a valid host address from within that subnet.

```
2621#config t
```

```
2621(config) int f0/0.1
```

```
2621(config-subif)# encapsulation isl 1
```

```
2621(config-subif)# ip address 172.16.10.1 255.255.255.0
```

```
2621(config-subif)# int f0/0.2
```

```
2621(config-subif)# encapsulation isl 2
```

```
VLAN 1 default 172.16.10.0/24
```

```
VLAN 2 sales 172.16.20.0/24
```

```
VLAN 3 marketing 172.16.30.0/24
```

```
VLAN 4 mis 172.16.40.0/24
```

```
2621(config-subif)# ip address 172.16.20.1 255.255.255.0
```

```
2621(config-subif)# int f0/0.3
```

```
2621(config-subif)# encapsulation isl 3
```

```
2621(config-subif)# ip address 172.16.30.1 255.255.255.0
```

```
2621(config-subif)# int f0/0.4
2621(config-subif)# encapsulation isl 4
2621(config-subif)# ip address 172.16.40.1 255.255.255.0
2621(config-subif)#exit
2621(config)#int f0/0
2621(config-if) no shutdown
```

After setting the encapsulation and IP address for VLAN 1, I did the same configurations for VLANs 2, 3, and 4. Notice, however, that each sub interface is in a separate subnet.

---

17) What is CDP? Illustrate how to configure CDP on the CISCO Switches.

ANS : DP works with all Cisco devices, including the Catalyst 1900 switch. The output on the

1900 switch looks like this:

```
switch#sh cdp
```

Global CDP information: CDP version: 2

Sending CDP packets every 60 seconds

sending a hold time value of 180 seconds

```
#
```

Notice that both the router and the switch have a CDP timer of 60 seconds and a hold time of 180 seconds. This means that CDP information received from neighbour routers will be kept for 180 seconds. If the router or switch does not hear from the neighbour again before the hold time expires, the information will be discarded. You can change the timers on both devices with the cdp timer and cdp hold time commands from global configuration mode:

```
switch#config t
```

Enter configuration commands, one per line.

End with CNTL/Z switch(config)#cdp ?

advertise-v2                      CDP sends version-2 advertisements

Hold time Specify the hold time (in sec) to be sent in packets

Timer Specify the rate at which CDP packets are sent (in sec)

At this point, you can change the timer and hold time on the 1900 switch, as follows:

```
switch(config)#cdp timer 90
```

```
switch(config)#cdp hold time 240
```

---

## **TEN MARKS**

1)What is ISL Routing? What is its advantage? Demonstrate an ISL routing on a switched network having 4 vlans defined

ANS : In networking, ISL (Inter-Switch Link) routing is a protocol used to facilitate communication between switches in a switched network, primarily in the context of Cisco switches. It's a protocol used for VLAN (Virtual Local Area Network) tagging and allows for the transportation of multiple VLAN traffic between switches.

Advantages of ISL routing include:

1. \*VLAN Tagging:\* ISL allows the tagging of VLAN information within Ethernet frames, enabling the transmission of traffic from multiple VLANs across a single link between switches.

2. \*Interoperability:\* ISL was widely used in Cisco environments and supported by older Cisco switches, facilitating communication and VLAN configuration across these devices.

However, it's important to note that ISL has largely been replaced by the IEEE 802.1Q standard, which is an open standard for VLAN tagging and is more widely supported.

To support ISL routing on one FastEthernet interface, the router's interface is divided into logical interfaces (subinterfaces), one for each VLAN.

Configuring ISL Routing Rout

Since we have four VLANs, we need four subinterfaces.

Each one of the VLANs is a separate subnet

Following subnet we will use for each vlan

VLAN 1 default 172.16.10.0/24

VLAN 2 sales 172.16.20.0/24

VLAN 3 marketing 172.16.30.0/24

VLAN 4 mis 172.16.40.0/24

Each of the hosts in their VLAN must use the same subnet addressing

To configure the router-on-a-stick for inter-VLAN routing, you need to complete three steps

1)Enable ISL trunking on the switch port the router connects to

1) Enable ISL encapsulation on the router's sub interface.

1) Assign an IP address to the sub interface

Createing a sub-interface

```
2621#config t
```

```
2621(config) int f0/0.1
```

```
2621(config-subif)#
```

To configure ISL routing on a sub interface, use the command encapsulation isl [vlan-number]

```
2621(config-subif)# encapsulation isl 1
```

Assign an IP address to the sub interface.

```
2621(config-subif)# ip address 172.16.10.1  
255.255.255.0
```

FOR VLAN 1

```
2621#config t
```

```
2621(config) int f0/0.1
```

```
2621(config-subif)# encapsulation isl 1
```

```
2621(config-subif)# ip address 172.16.10.1  
255.255.255.0
```

FOR VLAN 2

```
2621#config t
```

```
2621(config) int f0/0.2
```

```
2621(config-subif)# encapsulation isl 2
```

```
2621(config-subif)# ip address 172.16.20.1  
255.255.255.0
```

FOR VLAN 3

```
2621#config t
```

```
2621(config) int f0/0.3
```

```
2621(config-subif)# encapsulation isl 3
```

```
2621(config-subif)# ip address 172.16.30.1  
255.255.255.0
```

FOR VLAN 4

```
2621#config t
```

```
2621(config) int f0/0.4
```

```
2621(config-subif)# encapsulation isl 4
```

```
2621(config-subif)# ip address 172.16.40.1  
255.255.255.0
```

```
2621(config)#int f0/0
```

```
2621(config-if) no shutdown
```

Notice, however, that each sub interface is in a separate subnet

Remember, ISL is an older protocol and might not be supported in newer Cisco switches or software versions. The more commonly used and widely supported protocol for VLAN tagging is IEEE 802.1Q. Always refer to the specific switch documentation or Cisco's official resources for accurate commands and configurations as per your switch model and software version.

---

2)What is MAC address table? What are the different types of entries in this table? Give its significance

ANS : The switches create a MAC table that includes dynamic, permanent, and static addresses.

This filter table is created by hosts sending a frame and by the switch learning the source MAC address and from which segment and port it was received.

The switch keeps adding new MAC addresses that are sent on the net-work into the MAC filter table. As hosts are added or removed, the switch dynamically updates the MAC filter

table. If a device is removed, or if it is not connected to the switch for a period of time, the switch will age out the entry.

You can see the switch's filter table by using the command `show mac-address-table`. The following output shows the information received when using the `show mac-address-table` command.

```
Todd1900EN#sh mac-address-table
Number of permanent addresses : 0
Number of restricted static addresses : 0
Number of dynamic addresses : 4
Address Dest Interface Type Source
Interface List
00A0.246E.0FA8 Ethernet 0/2 Dynamic All
0000.8147.4E11 Ethernet 0/5 Dynamic All
0000.8610.C16F Ethernet 0/1 Dynamic All
00A0.2448.60A5 Ethernet 0/4 Dynamic All
```

The addresses in the table above are from the four hosts connected to my 1900 switch. They are all dynamic entries, which means the switch looked at the source address of a frame as it entered the switch interface, and it placed that address in the filter table. Notice that I have hosts in interfaces 1, 2, 4, and 5.

The Catalyst 1900 switch can store up to 1024 MAC addresses in the filter table. If the MAC filter table gets full, the switch will flood all new addresses until one of the existing entries gets aged out.

You can also clear the MAC filter table by using the `clear mac-address-table` command. You can clear dynamic, permanent, and restricted static addresses. The switch output below shows the different options available when using the `clear macaddress-table` command.

```
#clear mac-address-table ?
dynamic Clear 802.1d dynamic address
permanent Clear 802.1d permanent addresses
restricted Clear 802.1d restricted static address
```

---

3) Give the different methods of security implementation on Switched Networks  
Not found answer