CCNP SWITCH

Student Lab Manual

→

NETWORKERS HOME

IGNITE YOUR GENIUS

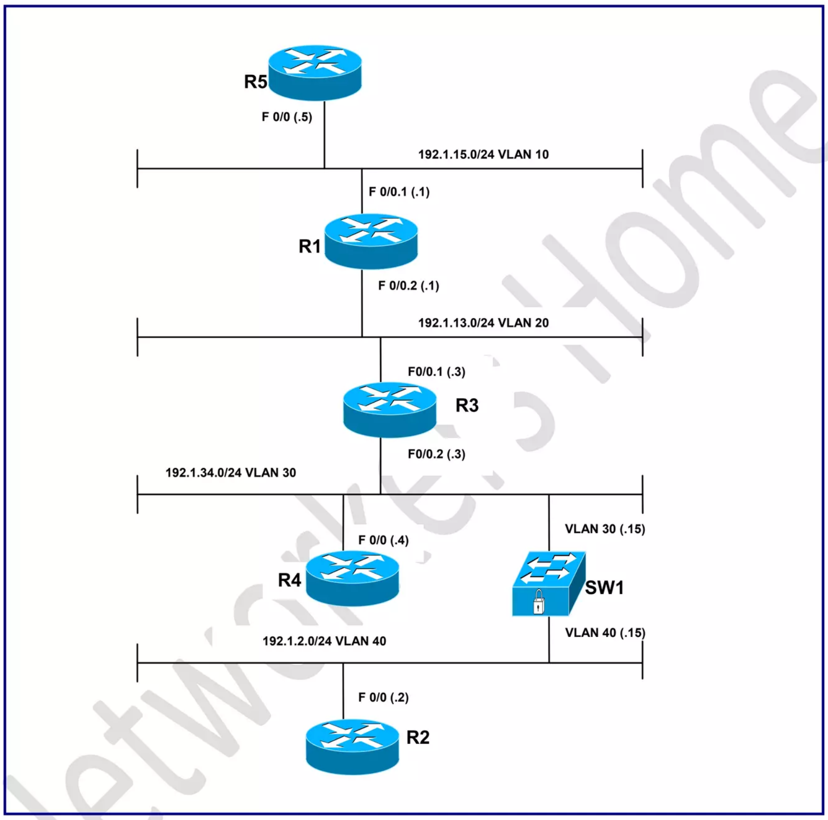
Web : www.networkershome.com Email : info@networkershome.com

NETWORKERS HOME

IGNITE YOUR GENIUS

CCNP SWITCH WORKBOOK
Module: 01 to 20

Lab 1- VTP, Trunking, VLANs and Inter-VLAN Routing



Task 1

Configure the Switches with Hostnames of SW1 and SW2 respectively.

SW1	**SW2**
Hostname SW1	Hostname SW2

Task 2
Configure both switches to be in a VTP Domain CISCO. SW1 should be configured as a Server and SW2 as a Client.

SW1	SW2
VTP domain CISCO VTP mode Server	VTP domain CISCO VTP mode client

Task 3
The CISCO VTP Domain should be password protected using NETMET as the Password.

SW1	SW2
VTP password NETMET	VTP password NETMET

Task 4
Configure Trunking between SW1 and SW2 on all ports that connect the switches to each other. Use an Industry standard encapsulation mechanism.

SW1	SW2
Interface Range F0/XX – Fast0/YY Switchport Trunk Encap dot1q Switchport mode trunk	Interface Range F0/XX – Fast0/YY Switchport Trunk Encap dot1q Switchport mode trunk

Task 5
Create VLAN's based on the Diagram. Assign the appropriate ports to the appropriate VLAN's based on the Logical Diagram. Use an industry standard encapsulation wherever required.

SW1

```
VLAN 10
VLAN 20
VLAN 30
VLAN 40
!
interface F0/1 , F0/3
Switchport Trunk Encap dot1q
 Switchport mode trunk
!
interface F0/2
Switchport access vlan 40
```

```
 Switchport mode access
!
Interface F0/4
 Switchport access vlan 30
 Switchport mode access
!
Interface F0/5
 Switchport access vlan 10
 Switchport mode access
```

Task 6

Configure the Routers and SW1 with the Appropriate IP addresses based on the Logical Diagram.

R1 Interface F 0/0 No shut ! Interface F 0/0.1 Encapsulation dot1q 10 IP Address 192.1.15.1 255.255.255.0 ! Interface F0/0.2 Encapsulation dot1q 20 IP Address 192.1.13.1 255.255.255.0	**R2** Interface F 0/0 IP Address 192.1.2.2 255.255.255.0 No shut
R3 Interface F 0/0 No shut ! Interface F 0/0.1 Encapsulation dot1q 20 IP Address 192.1.13.3 255.255.255.0 ! Interface F0/0.2 Encapsulation dot1q 30 IP Address 192.1.34.3 255.255.255.0	**R4** Interface F 0/0 IP Address 192.1.34.4 255.255.255.0 No shut
R5 Interface F 0/0 IP Address 192.1.15.5 255.255.255.0 No shut	**SW1** IP Routing ! Interface VLAN 30 IP Address 192.1.34.15 255.255.255.0 !

	Interface VLAN 40 IP Address 192.1.2.15 255.255.255.0

Task 7

Configure a Loopback 0 interface on each Rotuer with an IP Address of X.X.X.X/8 (where X is the Router # - R1=1, R2=2 ....). Loopback 0 on SW1 as 15.15.15.15/8. Run RIP v2 on all the routers and SW1 such that all networks are reachable from all devices.

R1 Interface Loopback 0 IP Address 1.1.1.1 255.0.0.0 ! Router RIP Version 2 No auto-summary Network 192.1.15.0 Network 192.1.13.0 Network 1.0.0.0	**R2** Interface Loopback 0 IP Address 2.2.2.2 255.0.0.0 ! Router RIP Version 2 No auto-summary Network 192.1.2.0 Network 2.0.0.0
R3 Interface Loopback 0 IP Address 3.3.3.3 255.0.0.0 ! Router RIP Version 2 No auto-summary Network 192.1.13.0 Network 192.1.34.0 Network 3.0.0.0	**R4** Interface Loopback 0 IP Address 4.4.4.4 255.0.0.0 ! Router RIP Version 2 No auto-summary Network 192.1.34.0 Network 4.0.0.0
R5 Interface Loopback 0 IP Address 5.5.5.5 255.0.0.0 ! Router RIP Version 2 No auto-summary Network 192.1.15.0 Network 1.0.0.0	**SW1** Interface Loopback 0 IP Address 15.15.15.15 255.0.0.0 ! Router RIP Version 2 No auto-summary Network 192.1.34.0 Network 192.1.2.0 Network 15.0.0.0

Lab 2 – Configuring Etherchannels

Task 1

Configure the Trunk Ports connecting SW1 and SW2 to be part of an Etherchannel. The Etherchannel should use an Industry standard protocol.

SW1	**SW2**
Inteface F0/XX , F0/YY Channel-group 1 mode active	Inteface F0/XX , F0/YY Channel-group 1 mode active

Task 2

Configure the Load Balancing mechanism method to be done based on a combination of the Source and Destination IP.

SW1
Port-channel load-balance src-dst-ip
SW2
Port-channel load-balance src-dst-ip

Task 3

Verify the Etherchannel status.

SW1

Show etherchannel 1 port-channel

```
Port-channels in the group:
---------------------------
Port-channel: Po1 (Primary Aggregator)
------------
Age of the Port-channel = 00d:00h:01m:09s
Logical slot/port = 1/0 Number of ports = 0
HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = LACP
```

Explanation:

An **EtherChanne**l consists of individual Fast Ethernet or Gigabit Ethernet links bundled into a single logical link.

If a link within an EtherChannel fails, traffic previously carried over that failed link changes to the remaining links within the EtherChannel. A trap is sent for a failure, identifying the switch, the EtherChannel, and the failed link.

Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

NOTE: All interfaces in each Etherchannel must be the same speed and duplex, same trunking encapsulation or the same access vlan ID, also the STP cost for each port must be the same and none of the Etherchannel ports can be involved in SPAN, RSPAN configuration or neither 802.1X.

Understanding Port-Channel Interfaces

You create an EtherChannel for Layer 2 interfaces differently from Layer 3 interfaces. Both configurations involve logical interfaces.

- With **Layer 3** interfaces, you manually create the logical interface by using the **interface port-channel** global configuration command.
- With **Layer 2** interfaces, the logical interface is dynamically created.
- With both **Layer 3** and **2** interfaces, you manually assign an interface to the EtherChannel by using the channel-group interface configuration command. This command binds the physical and logical ports together

An **Etherchannel cannot** be configured in both the **PAgP** and **LACP** modes.

Lab 3 – Configuring MSTP

Task 1

Disable the Etherchannel configured in the previous lab on SW1 and SW2 to test MSTP.

SW1	**SW2**
Inteface F0/XX , F0/YY No Channel-group 1 mode active	Inteface F0/XX , F0/YY No Channel-group 1 mode active

Task 2

Configure Multi-instance of Spanning Tree on the switches as follows:

- ✓ There should be two instances of STP, instance 1 and 2
- ✓ Instance 1 should handle VLANs 10 and 20
- ✓ Instance 2 should handle VLAN 30 and 40
- ✓ SW1 should be the root bridge for the first instance
- ✓ SW2 should be the root bridge for the second instance
- ✓ MST configuration should use the following:
    - o Name : CISCO
    - o Revision : 1
- ✓ Instance 1 should use the lower Trunk Interface as the Primary forwarding port
- ✓ Instance 2 should use the lower Trunk Interface as the Primary forwarding port

SW1	**SW2**
Spanning-tree mode mst ! Spanning-tree mst configuration Revision 1 Name CISCO Instance 1 vlan 10,20 Instance 2 vlan 30,40 ! Spanning-tree mst 1 priority 0 Spanning-tree mst 2 priority 4096 ! Int F0/XX Spanning-tree mst 1 port-priority 0	Spanning-tree mode mst ! Spanning-tree mst configuration Revision 1 Name CISCO Instance 1 vlan 10,20 Instance 2 vlan 30,40 ! Spanning-tree mst 1 priority 4096 Spanning-tree mst 2 priority 0 ! Int F0/YY Spanning-tree mst 1 port-priority 0

Lab 4 – Configuring SPAN/RSPAN

Task 1

There is a protocol analyzer connected to SW2 port F0/18. You received a request to monitor and analyze all packets for port F0/16 on SW1, configure the switches to accommodate this request.

SW1

```
Vlan 90
  Remote-span
!
Monitor session 1 source interface F0/16
Monitor session 1 destination remote vlan 90
```

SW2

```
Monitor session 1 source vlan 90
Monitor session 1 destination interface F 0/18
```

Lab 5 – Configuring VLAN ACLs (VACL)

Task 1

You have been requested to implement the following policy on SW1:

- ✓ Deny IGMP in VLAN 10
- ✓ Deny TFTP in VLAN 20
- ✓ Deny ICMP and TFTP in VLAN 30
- ✓ There is a MAC address 0001.0012.2222 trying to attack VLAN 40. Block this MAC address from accessing any device in VLAN 40.

SW1

```
Access-list 101 permit igmp any any
!
Access-list 102 permit udp any any eq 69
!
Access-list 103 permit igmp any any
Access-list 103 permit udp any any eq 69
!
Mac access-list extended MAC-ACL
 Permit host 0001.0012.2222 any
!
Vlan access-map VLAN10 10
 Match ip addr 101
 Action drop
Vlan access-map VLAN10 100
!
Vlan access-map VLAN20 10
 Match ip addr 102
 Action drop
Vlan access-map VLAN20 100
!
Vlan access-map VLAN30 10
 Match ip addr 103
 Action drop
Vlan access-map VLAN30 100
!
Vlan access-map VLAN40 10
 Match mac address MAC-ACL
 Action drop
Vlan access-map VLAN40 100
!
Vlan filter VLAN10 vlan-list 10
Vlan filter VLAN20 vlan-list 20
Vlan filter VLAN30 vlan-list 30
Vlan filter VLAN40 vlan-list 40
```

Lab 6 – Configuring Port Security

Task 1

Configure VLAN 50 on SW1. Configure Ports F 0/3 and F0/4 on SW2 in VLAN 50. Configure SW2 such that only R3 F 0/1 and R4 F 0/1 can connect to ports F 0/3 and F0/4 on SW2 respectively. If another port tries to connect to these ports, the ports should be error disabled.

SW1

```
VLAN 50
```

SW2

```
Interface F 0/3
 Switchport mode access
 Switchport access vlan 50
 Switchport port-security
 Switchport port-security mac xxxx.xxxx.xxxx
!
Interface F 0/4
 Switchport mode access
 Switchport access vlan 50
 Switchport port-security
 Switchport port-security mac xxxx.xxxx.xxxx
```

Task 2

Configure F 0/5 – F 0/8 in VLAN 50 on SW2. Enable Port Security for these ports such that only 1 MAC address can be connected to them. You would like to learn the MAC address dynamically.

SW2

```
Int range F 0/5 – F 0/8
Switchport mode access
Switchport access vlan 50
Switchport port-security
Switchport port-security mac-address sticky
```

Task 3

Configure F 0/15 also in VLAN 50 on SW2. Enable Port security for these ports such that 5 MAC addresses can be connected to this port. The first 2 MAC addresses that are allowed to connect are 0001.1010.AB12 and 0001.1010.AB13. The remaining 3 can be learned dynamically.

SW2

```
Int F 0/15
Switchport mode access
Switchport access vlan 50
Switchport port-security
Switchport port-security max 5
Switcport port-security mac-address 0001.1010.AB12
Switcport port-security mac-address 0001.1010.AB13
Switcport port-security mac-address sticky
```

Lab 7 – Regular and Smart Macros

Task 1

Configure switchports on SW1 that connect to R2, R4 and R5 as Regular Macro with a name of RP.

SW1

```
Define interface-range RP F0/2 , F 0/4,  F0/5
```

The above command defines a range of ports on the switch and names them Router-Ports, in some documentation this is referred to as a regular macro

Task 2

Configure the RP Ports with Port Security. SW1 should learn the MAC addresses dynamically. Use a Smart Macro to accomplish this task.

SW1

```
Macro name Port-Secure
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
@
!
Interface range macro RP
 Macro apply Port-Secure
!
```

The above configuration configures a smartport macro. A smartport macro is started by the "Macro name" command and then followed by an arbitrary name that is assigned to the macro.

Once that command is entered, a message is displayed in the next command line. This message tells us to use the @ sign in order to end this macro.

To run the Macro, use the Macro Apply command under the interface.

Lab 8 – Configuring Dot1X Authentication

Task 1

The PCs that are connected or will be connected to SW1 ports F0/17 – 18 should get authenticated before they are allowed access to the network. These PC's belong to VLAN 40. This authentication should use a RADIUS server located at 192.1.2.100 using "cisco" as the key.

```
SW1

Aaa new-model
!
aaa authentication dot1x default group radius
!
Dot1x system-auth-control
!
Interface range F 0/17 – 18
 Switch mode access
 Swithcport access vlan 40
 Dot1x port-control auto
```

Task 2

If the PC does not support Dot1X authentication, it should be put into VLAN 60. If the user fails authentication, it should be put into VLAN 61.

```
SW1

VLAN 60
VLAN 61
!
Interface range F 0/17 – 18
  Dot1x guest-vlan 60
  Dot1x auth-fail vlan 61
```

Lab 9 – Configuring Storm Control

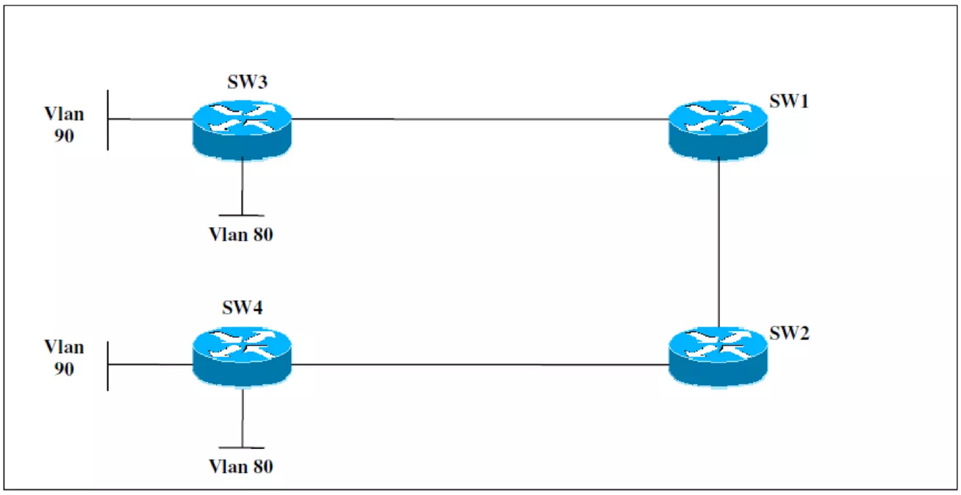
Task 1

Configure SW2 port F0/14 such that broadcast and multicast traffic do not use more than 50% of the Interface bandwidth.

SW2

```
Interface F0/14
Storm-control broadcast level 50.00
Storm-control multicast level 50.00
```

Lab 10 – Configuring QinQ Tunneling



Interface IP Address Configuration

SW3 (Customer Switch)

Interface	IP Address	Subnet Mask
Int SVI 80	150.1.80.3	255.255.255.0
Int SVI 90	150.1.90.3	255.255.255.0

SW4 (Customer Switch)

Interface	IP Address	Subnet Mask
Int SVI 80	150.1.80.4	255.255.255.0
Int SVI 90	150.1.90.4	255.255.255.0

Task 1

Only Keep 1 Trunk link up between the switches. Also, make sure only the following links are up:

- SW1 – SW3
- SW1 – SW2
- SW2 – SW4

SW1

```
!
Interface range F0/X – Y
 Shutdown
 Description All trunk ports on SW1
!
Interface range F 0/A  , F 0/B
 No shutdown
 Description One Trunk each towards SW2 and SW3
```

SW2

```
!
Interface range F0/X – Y
 Shutdown
 Description All trunk ports on SW2
!
Interface range F 0/A  , F 0/B
 No shutdown
 Description One Trunk each towards SW1 and SW4
```

SW3

```
!
Interface range F0/X – Y
 Shutdown
 Description All trunk ports on SW3
!
Interface F 0/A
 No shutdown
 Description One Trunk link towards SW1
```

SW4

```
!
Interface range F0/X – Y
 Shutdown
 Description All trunk ports on SW4
!
Interface F 0/A
 No shutdown
 Description One Trunk link towards SW2
```

Task 2

Configure Q-in-Q tunneling on SW1 and SW2 in such a way that allows customer VLANs to cross the trunk linkds without alteration in the Customer switches. Also, allow VLAN overlapping between other Service Provider Customers. Change the MTU size to accommodate Q-in-Q tunneling. Assign the Customer to a VLAN 120.

SW1

```
System mtu 1504
!*** requires a reload***
VLAN 120
!
Interface F0/A
 Description Trunk ports connecting towards SW3-Customer Switch
Switchport access vlan 120
Switchport mode dot1q-tunnel
!
Interface F0/B
 Description Trunk port towards the other Service Provider Switch(s)
 Switchport trunk encap dot1q
 Switchport mode trunk
```

SW2

```
System mtu 1504
! *** requires a reload***
VLAN 120
!
Interface F0/A
 Description Trunk ports connecting towards SW4-Customer Switch
Switchport access vlan 120
Switchport mode dot1q-tunnel
!
Interface F0/B
 Description Trunk port towards the other Service Provider Switch(s)
 Switchport trunk encap dot1q
 Switchport mode trunk
```

Task 3

Configure the Customer Side Switches with Dot1Q trunking encapsulation.

SW3

```
Interface F0/B
 Description Trunk port towards the Service Provider Cloud
 Switchport trunk encap dot1q
 Switchport mode trunk
```

SW4

```
Interface F0/B
 Description Trunk port towards the Service Provider Cloud
 Switchport trunk encap dot1q
 Switchport mode trunk
```

Task 4

Configure QinQ and Layer Protocol Forwarding (metro) in such a way that allows switches to forward CDP and VTP customer's frames transparently. Configure switches SW1 and SW2 ports facing SW3 and SW4 respectively.

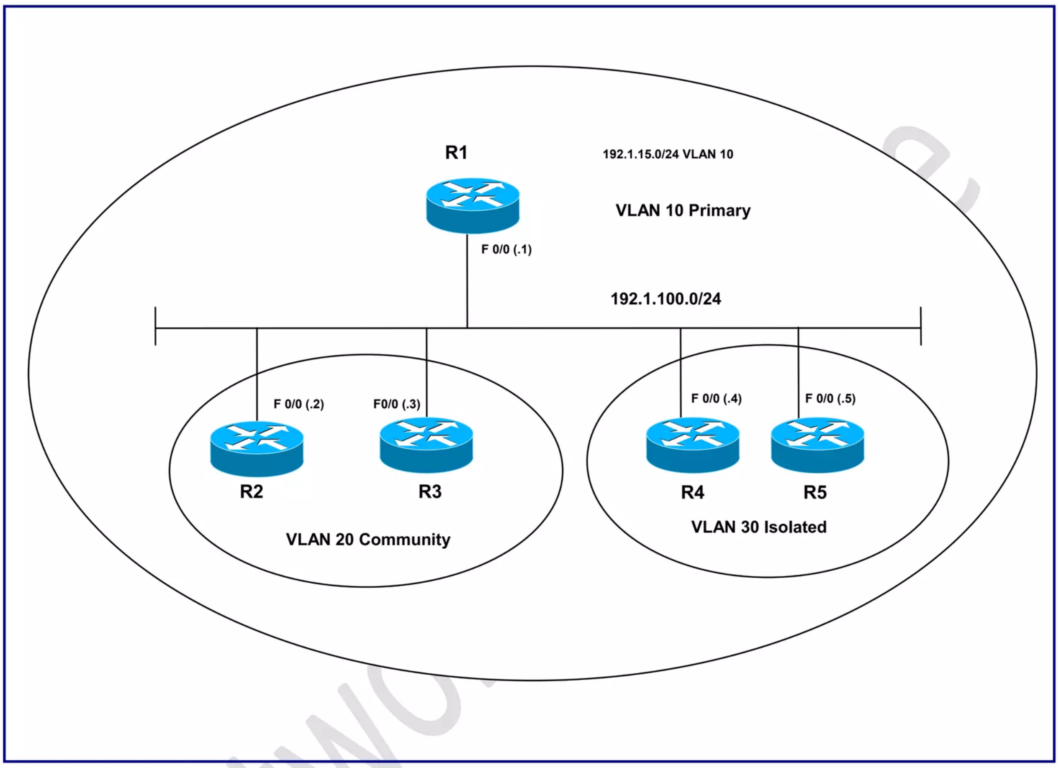
SW1

```
Interface F0/A
 Description Trunk ports connecting towards SW3-Customer Switch
 L2protocol-tunnel cdp
 L2protocol-tunnel vtp
```

SW2

```
Interface F0/A
 Description Trunk ports connecting towards SW4-Customer Switch
 L2protocol-tunnel cdp
 L2protocol-tunnel vtp
```

Lab 11 – Configuring Private VLANs



Interface IP Address Configuration

R1

Interface IP	Address	Subnet Mask
F 0/0	192.1.100.1	255.255.255.0

R2

Interface IP	Address	Subnet Mask
F 0/0	192.1.100.2	255.255.255.0

R3

Interface IP	Address	Subnet Mask
F 0/0	192.1.100.3	255.255.255.0

R4

Interface IP	Address	Subnet Mask
F 0/0	192.1.100.4	255.255.255.0

R5

Interface IP	Address	Subnet Mask
F 0/0	192.1.100.5	255.255.255.0

Task 1

Configure VTP Transparent mode in SW1 and create the following configuration:
Vlan 10 as Private-Vlan **Primary**
Vlan 20 as Private-Vlan **Community**
Vlan 30 as Private-Vlan **Isolated**

SW1

```
Vtp mode transparent
!
Vlan 10
Private-vlan primary
!
Vlan 20
Private-vlan community
!
Vlan 30
Private-vlan isolated
!
Vlan 10
Private-vlan association add 20, 30
```

Task 2

Configure SW1 such that the following is accomplished keeping the VLAN designations from Task1:

- R1 should be able to communicate to all other devices.
- R2 and R3 should be able to communicate to each other and R1 but should not have access to R4 or R5.
- R4 and R5 should only be able to communicate to R1. They should not be able to communicate to each other or R2 or R3.

SW1

```
Interface F0/1
Switchport mode private-vlan promiscuous
Switchport private-vlan mapping 10 add 20 , 30
!
Interface range F0/2 – 3
Switchport mode private-vlan host
Switchport private-vlan host-assoc 10 20
!
Interface range F0/4 – 5
Switchport mode private-vlan host
Switchport private-vlan host-assoc 10 30
```

Explanation:

Private VLANs provide Layer 2 isolation between ports within the same private VLAN. There are three types of private VLAN ports:

• **Promiscuous**—A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN.

• **Isolated**—An isolated port has complete Layer 2 separation from other ports within the same private VLAN except for the promiscuous port. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports.

• **Community**—Community ports communicate among themselves and with their promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities or isolated ports within their private VLAN.

NOTE: Because trunks can support the VLANs carrying traffic between isolated, community, and promiscuous ports, isolated and community port traffic might enter or leave the switch through a trunk interface.

Private VLAN ports are associated with a set of supporting VLANs that are used to create the private VLAN structure. A private VLAN uses VLANs three ways:

• **Primary VLAN**—Carries traffic from promiscuous ports to isolated, community, and other promiscuous ports.

• **Isolated VLAN**—Carries traffic from isolated ports to promiscuous ports.

• **Community VLAN**—Carries traffic between community ports and to promiscuous ports. You can configure multiple community VLANs in a private VLAN.

NOTE: Isolated and **community** VLANs are both called **secondary VLANs**.
A promiscuous port can serve only one primary VLAN and can serve as many isolated or community VLANs as desired

Lab 12 – Tuning STP Startup Times

Task 1
Create a VLAN 50 on SW1. Assign ports F 0/6 – F 0/8 to VLAN 50.

```
SW1

VLAN 50
!
Interface range F 0/6 – 8
 Switchport access vlan 50
 Switchport mode access
```

Task 2
Users in Vlan 50 are complaining about the time it usually takes for an interface to come up after they have plugged in the network cable. Configure the TOTAL link startup delay until the port becomes forwarding to 16 seconds. Configure SW1 to accomplish this without jumping any state.

```
SW1

Spanning-tree vlan 50 forward-time 8
```

Output of command:

```
SW1

show spanning-tree vlan 50 brief
VLAN50
Spanning tree enabled protocol ieee
Root ID Priority 8192
Address cc08.01f8.000c
Cost 32
Port 50 (FastEthernet0/6)
Hello Time 2 sec Max Age 20 sec Forward Delay 8 sec
Bridge ID Priority 32768
Address cc06.0a4c.000c
Hello Time 2 sec Max Age 20 sec Forward Delay 8 sec
Aging Time 0
Interface Designated
………
```

Explanation:

Forwarding delay is the time spent by a port in the **learning** and **listening** states.

By default it has a value of 15 seconds so a normal port without portfast enable on it usually takes 50 seconds to start forwarding packets because it goes through learning (15 seconds) plus listening (15 seconds) and maximum age time (which is 20 seconds by default) when changing the forwarding delay to 8 the time the port for the first time a desktop is plugged into a port in a switch it would take 8 + 8 + 20 (if it's using the default value) so it would takes 36 seconds instead of 50 seconds in that case.

Lab 13 – Configuring Port-Fast

Task 1

Configure the port range from F0/1 – 6 on SW1 in a way that, the link will come up as soon as someone plug in a network cable into some of these ports bypassing STP learning/listening states.

```
SW1

Interface range F0/1 - 6
Spanning-tree portfast
```

Output of command:

```
SW1

show spanning-tree interface F0/1 portfast

VLAN10 enabled.
```

Explanation:

After a port on the switch has linked and joined the bridge group, STP runs on that port. A port that runs STP can be in one of five states:

- **blocking**
- **listening**
- **learning**
- **forwarding**
- **disabled**

STP dictates that the port starts out blocking, and then immediately moves through the listening and learning phases.

By default, the port spends approximately 15 seconds listening and 15 seconds learning.

During the listening state, the switch tries to determine where the port fits in the spanning tree topology. The switch especially wants to know whether this port is part of a physical loop. If the port is part of a loop, the port can be chosen to go into blocking mode.

The **blocking state** means that the port does not send or receive user data in order to eliminate loops.
If the port is not part of a loop, the port proceeds to the learning state, in which the port learns which MAC addresses live off this port. This entire STP initialization process takes about 30 seconds.

If you connect a workstation or a server with a single NIC card or an IP phone to a switch port, the connection cannot create a physical loop. These connections are considered leaf nodes. There is no reason to make the workstation wait 30 seconds while the switch checks for loops if the workstation cannot cause a loop.

Cisco added the PortFast or fast-start feature. With this feature, the STP for this port assumes that the port is not part of a loop and immediately moves to the forwarding state and does not go through the blocking, listening, or learning states. This command does not turn STP off. This command makes STP skip a few initial steps (unnecessary steps, in this circumstance) on the selected port.

NOTE: Never use the PortFast feature on switch ports that connect to other switches, hubs, or routers. These connections can cause physical loops, and spanning tree must go through the full initialization procedure in these situations. A spanning tree loop can bring your network down. If you turn on PortFast for a port that is part of a physical loop, there can be a window of time when packets are continuously forwarded (and can even multiply) in such a way that the network cannot recover.

At the global level, you enable BPDU guard on Port Fast-enabled NNIs by using the **spanning-tree portfast bpduguard default** global configuration command. Spanning tree shuts down NNIs that are in a Port Fast-operational state if any BPDU is received on those NNIs.

In a valid configuration, Port Fast-enabled NNIs do not receive BPDUs. Receiving a BPDU on a Port Fastenabled NNI signals an invalid configuration, such as the connection of an unauthorized device,and the BPDU guard feature puts the interface in the error-disabled state.

At the interface level, you enable BPDU guard on any NNI by using the **spanning-tree bpduguard enable** interface configuration command without also enabling the Port Fast feature. When the NNI receives a BPDU, it is put in the error-disabled state.

Lab 14 - Configuring BPDU Guard

Task 1

The IT departament just found out that someone in the lobby area just plugged in a switch into port F0/6 on SW1. Configure a command globally on SW1 that if someone connects a hub or a switch to any of the access ports, the port will be disabled. Also make sure that after 4 minutes the disabled port comes up automatically

SW1

```
Spanning-tree portfast bpduguard
!
Errdisable recovery cause bpduguard
Errdisable recovery interval 240
```

Output of command:

SW1

```
show errdisable recovery

ErrDisable Reason Timer Status
----------------- --------------
udld Disabled
bpduguard Enabled
rootguard Disabled
pagp-flap Disabled
dtp-flap Disabled
link-flap Disabled
Timer interval: 240 seconds
Interfaces that will be enabled at the next timeout:

show spanning-tree summary
Root bridge for: VLAN1, VLAN10, VLAN13, VLAN16, VLAN19, VLAN20, VLAN30

PortFast BPDU Guard is enabled
UplinkFast is disabled
BackboneFast is disabled
…
```

Explanation:

Port Fast-enabled ports do not receive **BPDUs**. Receiving a BPDU on a Port Fast-enabled port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state.

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking ports. Configure Port Fast only on ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled port moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can also configure bpduguard under an interface using the command **"spanning-tree bpduguard".**

Lab 15 – Configuring BPDU Filter

Task 1

Configure SW2 port F0/15 such that this port won't send or receive any BDPU packets.

```
SW2

Interface F0/15
 Spanning-tree bpdufilter enable
```

Explanation:

BPDU Filtering

The **BPDU filtering** feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.

At the **global level**, you can enable BPDU filtering on Port Fast-enabled interfaces by using the **spanning-tree portfast bpdufilter default** global configuration command. This command prevents interfaces that are in a Port Fast-operational state from sending or receiving BPDUs.

The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

At the **interface level**, you can enable BPDU filtering on any interface by using the **spanning-tree bpdufilter enable** interface configuration command without also enabling the Port Fast feature. This command prevents the interface from sending or receiving BPDUs.

Task 2

Configure SW1 such that any port configured with portfast should be limited from sending or receiving BPDU. Don't use any interface level command to accomplish this.

```
SW1

Spanning-tree portfast bpdufilter default
```

Output of command:

```
SW

show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is enabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short
```

Lab 16 – Configuring UplinkFast

Task 1

On SW1 configure a feature to improve the uplinks and make sure that if a root port has failed, the switch will choose a new root port and put it directly to FORWARDING state.

```
SW1

Spanning-tree uplinkfast
```

Output of command:

```
SW1

show spanning-tree uplinkfast

UplinkFast is enabled
Station update rate set to 150 packets/sec.
UplinkFast statistics
-----------------------
Number of transitions via uplinkFast (all VLANs) : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0
Name Interface List
.....
```

Explanation:

UplinkFast provides fast convergence after a spanning-tree topology change and achieves load balancing between redundant links using uplink groups. An uplink group is a set of ports (per VLAN), only one of which is forwarding at any given time. Specifically, an uplink group consists of the root port (which is forwarding) and a set of blocked ports, except for self-looping ports. The uplink group provides an alternate path in case the currently forwarding link fails.

UplinkFast is most useful in wiring-closet switches. This feature may not be useful for other types of applications.

NOTE: In other words **UplinkFast** is used to designate a **Backup Root Port** in case of **direct failure** of a link.

Lab 17 – Configuring Backbone Fast

Task 1

Configure SW1 and make sure that if an inferior BPDU is received on a root port or blocked port this inferior BPDUs is ignored on those ports.

```
SW1

Spanning-tree backbonefast
```

Output of command:

```
SW1
show spanning-tree summary

Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is enabled
Loopguard Default is disabled
UplinkFast is enabled
BackboneFast is enabled
Configured Pathcost method used is short
……
-----------------------
Number of transitions via uplinkFast (all VLANs) : 0
Number of proxy multicast addresses transmitted (all VLANs) : 0
BackboneFast statistics
-----------------------
Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs) : 0
Number of RLQ request PDUs received (all VLANs) : 0
Number of RLQ response PDUs received (all VLANs) : 0
Number of RLQ request PDUs sent (all VLANs) : 0
Number of RLQ response PDUs sent (all VLANs) : 0
```

Explanation:

BackboneFast is initiated when a root port or blocked port on a switch eceives inferior BPDUs from its designated bridge.

An **inferior BPDU** identifies one switch as both the root bridge and the designated bridge. When a switch receives an inferior BPDU, it indicates that a link to which the switch is not directly connected (an indirect link) has failed (that is, the designated bridge has lost its connection to the root bridge). Under normal spanning-tree rules, the switch ignores inferior BPDUs for the configured maximum aging time, as specified by the agingtime variable.

The switch tries to determine if it has an alternate path to the root bridge. If the **inferior BPDU** arrives on a blocked port, the root port and other blocked ports on the switch become alternate paths to the root bridge. (Self-looped ports are not considered alternate paths to the root bridge.)If the inferior BPDU arrives on the root port, all blocked ports become alternate paths to the rootbridge.

If the inferior BPDU arrives on the root port and there are no blocked ports, the switch assumes that it has lost connectivity to the root bridge, causes the maximum aging time on the root to expire, and becomes the root switch according to normal spanning-tree rules.

If the switch has alternate paths to the root bridge, it uses these alternate paths to transmit a new kind of PDU called the **Root Link Query PDU**. The switch sends the **Root Link Query PDU** out all alternate paths to the root bridge.

If the switch determines that it still has an alternate path to the root, it causes the maximum aging time on the ports on which it received the inferior BPDU to expire. If all the alternate paths to the root bridge indicate that the switch has lost connectivity to the root bridge, the switch causes the maximum aging times on the ports on which it received an inferior BPDU to expire.

If one or more alternate paths can still connect to the root bridge, the switch makes all ports on which it received an inferior BPDU its designated ports and moves them out of the blocking state (if they were in blocking state), through the listening and learning states, and into the forwarding state.

Lab 18 – Configuring Root Guard

Task 1

Configure the ports that connect SW1 to SW2 in such a way that if for some reason the spanning-tree causes one of those ports to be selected as root port, the port transition to a root-inconsistent (blocked) state.

```
SW1

Interface range F0/X – Y
 Description Connection towards SW2
 Spanning-tree guard root
```

Explanation:

The Layer 2 network of a service provider (SP) can include many connections to switches that are not owned by the SP. In such a topology, the spanning tree can reconfigure itself and select a customer switch as the root switch,

You can avoid this situation by enabling root guard on SP switch interfaces that connect to switches in your customer's network. If spanning-tree calculations cause an interface in the customer network to be selected as the root port, root guard then places the interface in the rootinconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root.

If a switch outside the SP network becomes the root switch, the interface is blocked (rootinconsistent state), and spanning tree selects a new root switch. The customer's switch does not become the root switch and is not in the path to the root.

If the switch is operating in multiple spanning-tree (MST) mode, root guard forces the interface to be a designated port. If a boundary port is blocked in an internal spanning-tree (IST) instance because of root guard, the interface also is blocked in all MST instances. A boundary port is an interface that connects to a LAN, the designated switch of which is either an 802.1D switch or a switch with a different MST region configuration.

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. VLANs can be grouped and mapped to an MST instance. You can enable this feature by using the **spanning-tree guard root** interface configuration command.

Lab 19 – DHCP Snooping & DAI

Task 1

Configure DHCP Snooping on Switch1. It should be enabled for VLAN 50. It should maintain a MAC-IP database based on the Addresses assigned to DHCP Clients from DHCP Servers.

```
SW1

IP DHCP snooping
IP DHCP snooping vlan 50
```

Task 2

The DHCP server resides on the F 0/16 on SW1. Assign this port to VLAN 50.

```
SW1

Interface F 0/16
 Switchport mode access
 Switchport access vlan 50
```

Task 3

Make sure the switch only allows DHCP replies from port F 0/16 on SW1.

```
SW2

Interface F 0/16
 Ip dhcp snooping trust
```

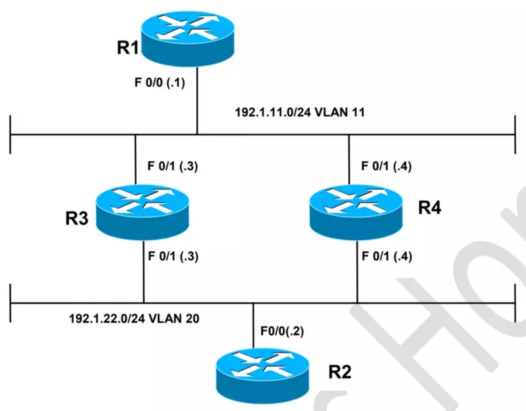
Task 4

Configure SW1 such that it intercepts all packets received on untrusted ports. It should verify valid IP-MAC mappings against the DHCP Snooping Database. If it does not match, it should drop the packets. It should be enabled on VLAN 50.

```
SW1

Ip arp inspection vlan 50
!
Interface F 0/16
Ip arp inspection trust
```

Lab 20 – Configuring HSRP



Interface IP Address Configuration

R1

Interface IP	Address	Subnet Mask
F 0/0	192.1.11.1	255.255.255.0

R2

Interface IP	Address	Subnet Mask
F 0/0	192.1.22.2	255.255.255.0
Loopback 0	2.2.2.2	255.0.0.0

R3

Interface IP	Address	Subnet Mask
F 0/0	192.1.22.3	255.255.255.0
F 0/1	192.1.11.3	255.255.255.0
Loopback 0	3.3.3.3	255.0.0.0

R4

Interface IP	Address	Subnet Mask
F 0/0	192.1.22.4	255.255.255.0
F 0/1	192.1.11.4	255.255.255.0
Loopback 0	4.4.4.4	255.0.0.0

Task 1

Configure EIGRP in AS 100 on R2, R3 and R4. Advertise the Loopback 0 and the physical links in EIGRP 100.

R2 Router EIGRP 100 No auto-summary Network 2.0.0.0 Network 192.1.22.0	**R3** Router EIGRP 100 No auto-summary Network 3.0.0.0 Network 192.1.22.0 Network 192.1.11.0
R4 Router EIGRP 100 No auto-summary Network 4.0.0.0 Network 192.1.22.0 Network 192.1.11.0	

Task 2

Configure HSRP between R3 and R4 on VLAN 11. Use .34 as the Virtual HSRP address. R3 should be the preferred Router. Have R1 point to the virtual HSRP address as the Default Gateway.

R3 Interface F 0/1 Standby 1 ip 192.1.11.34 Standby 1 priority 105 Standby 1 preempt	**R3** Interface F 0/1 Standby 1 ip 192.1.11.34
R1 IP route 0.0.0.0 0.0.0.0 192.1.11.34	

Testing:

- Type **Show standby** on R3 and R4.
- Which router is the Active HSRP Router?
- Which router is the Standby HSRP Router?
- Why?