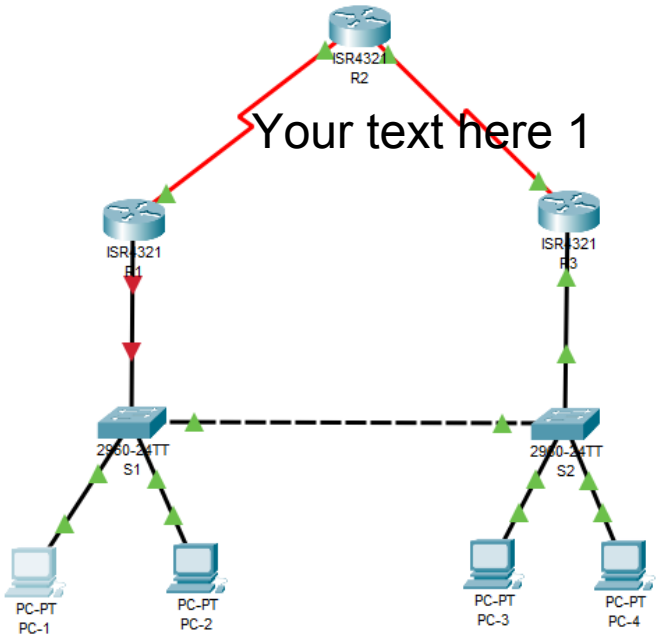
CCNA SRWE **Lab 3**

Team-No. 04 **Last Names:** Rubaiya Kabir Pranti

SRWE Module Group Exams **1-9 (Switch Config, SSH, VLAN, Trunk, STP, Ethertchannel, .. refresh)**
10-13 (LAN Security, WLAN)
14-16 (Static Routing)

VLAN, Trunk Refresher
Switch LAN Security
Static Routing



Homework

Lab Instructions

Task 1	VLAN, Trunk Refresher
Task 2	Switch LAN Security
Task 3	Static Routing

Deliverables and Due Dates

Homework / Lab Preparation

Part 1: Cisco IOS Basic Configuration Commands

a. Read the **Lab Instructions** of this Lab

b. Check the **IOS Command List**, provided for the Labs and review configuration commands.

Part 2: Switch Security

a) Switch Port Security

Why should you switch-off all unused ports?

To secure the network from unauthorized access need to switch-off all unused ports

Which command option helps not to edit each single interface?

(config)#int range f0/1-24
(config-if)#shutdown

For which type of switch port is it useful to limit the number of MAC addresses learned?

Dynamic secure MAC addresses are typically used in switch port

Which 3 options do you have in case of violation to switch port security?

Options are- Protect,Restrict and Shutdown

b) Secured Switch Trunks

Why is DTP dangerous for trunk ports?

DTP is a dynamic protocol that is available to help configure the switch ports. It might be active by default and in that case, the port is open to become a trunk if another device starts the negotiation, which poses a security risk.

How can you disable DTP on switch port f0/24?

```
S1(config)#  interface fa 0/24
S1(. . . )#  switchport nonegotiate
```

Which other security means do you have on trunk ports? Name in minimum 2 options.

There are two trunking protocols used on modern communication networks: Inter-Switch Link (ISL) from Cisco and the aforementioned nonproprietary IEEE 802.1Q

c) Spanning Tree Security

Describe how a man-in-the-middle attack on the STP protocol family can be performed.

By manipulating the STP or inserts a new STP device onto the network, attacker conduct an attack by spoofing the root bridge. Attackers can make their hosts appear as root bridges and capture all traffic for the immediate switched domain.

Configure STP security to prevent STP MITM attacks at switch access port F0/11.

```
S1(config)# int F0/11
S1(. . . )# spanning-tree portfast
            spanning-tree bpduguard enable
```

Part 3: Static Routing

a) Serial interface configuration

Configure the serial interface s0/0/1 with IP address of 10.0.01 / 25 and a clock rate of 125 kHz (is DCE) and shut-on the interface..

```
R1(config)# int s0/0/1
R1(. . . )# ip address 10.0.0.1 255.255.255.128
R1(. . . )# no shutdown
R1(. . . )# clock rate 125000
```

b) Static route configuration

Configure a static recursive route to network 192.168.0.0 / 24 via next hop 192.168.11.1.

```
R1(config)# ip route 192.168.0.0 255.255.255.0 192.168.11.1
```

Configure a directly connected static route to network 192.168.0.0 / 24 via exit interface g0/0.

```
R1(config)# ip route 192.168.0.0 255.255.255.0 g0/0
```

Configure a static default route via the next hop address 192.168.21.1.

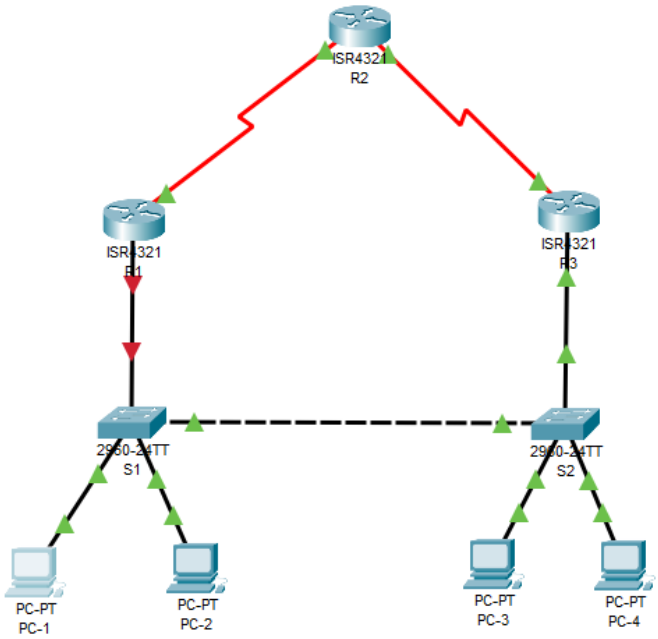
```
R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.21.1
```

Display the IPv4 routing table.

```
R1# show ip route
```

Task 1 – VLAN, Trunk Refresher

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/0.10	192.168.10.1	255.255.255.0	N/A
	G0/0/0.20	192.168.20.1	255.255.255.0	N/A
	G0/0/0.99	192.168.99.1	255.255.255.0	N/A
R3	G0/0/0.10	192.168.10.3	255.255.255.0	N/A
	G0/0/0.20	192.168.20.3	255.255.255.0	N/A
S1	VLAN99	192.168.99.101	255.255.255.0	192.168.99.1
S2	VLAN99	192.168.99.102	255.255.255.0	192.168.99.1
PC-1	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC-3	NIC	192.168.10.33	255.255.255.0	192.168.10.3
PC-2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC-4	NIC	192.168.20.24	255.255.255.0	192.168.20.3

VLAN Table

Switch	VLAN Number	VLAN Name	Access Port Membership	Network
S1	10	Admin	Fa0/2	192.168.10.0/24
	20	Sales	Fa0/3	192.168.20.0/24
	99	Management	Fa0/1	192.168.99.0/24
S2	10	Admin	Fa0/2	192.168.10.0/24
	20	Sales	Fa0/3	192.168.20.0/24
	99	Management	Fa0/1	192.168.99.0/24

Part 1: Build the Switched Network and Verify Connectivity

Step 1: Build topology in Packet Tracer.

COVID-19 Version: Build topology in **Packet Tracer**. Use and re-label the following devices:

a. Build the network with ISR4321 router, 2960 switches, and PCs in Packet Tracer. Rename the devices.

b. Cable the network according to the topology with straight-through TP cables and cross-over cables .

1. Ports F0/1 on both switches are interconnecting the switches
2. Port F0/2 and F0/3 connect PCs at switches S1 and S2
3. Port G0/1 of both switches connect to router R1 or router R3 respectively.

c. Implement serial interfaces NIM-2T at each router, and connect these interfaces by serial cables.

d. We will use the CLI window of the network devices directly for configurations.

Step 2: Configure PC hosts as shown in the topology and addressing table.

a. Configure IP address, net mask and default gateway for PC-1, PC-2, PC-3, and PC-4.

Step 3: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure device name

c. Assign **class** as the privileged EXEC encrypted password.

d. Assign **cisco** as the console password, enable login

e. Configure **logging synchronous** to prevent console messages from interrupting.

f. Configure password encryption

g. Save your running configuration in the startup configuration.

```
S1(config)# hostname S1
S1(config)# no ip domain-lookup
S1(config)# enable secret class
S1(config)# banner motd # Restricted Access. #

S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
```

Part 2: Create VLANs and Assign Switch Ports

Step 1: Create VLANs on the switches

a. Create VLANs 10, 20, and 99 on S1 and S2 according to the VLAN assignment list.

```
S1(config)# vlan 10
S1(config-vlan)# name Admin
S1(config)# vlan 20
S1(config-vlan)# name Sales
S1(config)# vlan 10
S1(config-vlan)# name Management
```

Step 2: Assign VLANs to Switch Access Ports

a. Assign switch ports to a VLAN according to the VLAN Table.

```
S1(config)# int f0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

Step 3: Create SVI Interface for VLAN99

a. Generate a switch IP address for the **Management VLAN 99** (virtual interface VLAN 99) on all switches according to the Addressing Table

```
S1(config)# interface vlan 99
S1(config-if)# ip address 192.168.99.101 255.255.255.0
S1(config-if)# no shutdown
```

Step 4: Configure a Default Gateway on Switches

a. Configure the **default gateway** for each switch according to the Addressing Table.

```
S1(config)# ip default-gateway 192.168.99.1
```

Step 5: Check VLAN and Connectivity

a. List your VLAN database on **S1** (**show vlan brief**).

Record, which switch ports are not in VLAN 1: Fa0/2,Fa0/3,Fa0/1

b. Check your interfaces on switch **S2** (**show ip interface brief)**.

Record the status of VLAN 99 interface: Vlan99 192.168.99.102 YES manual up

c. Check connectivity (ping) from S1 to S2 in VLAN 99. Connectivity (y/n)? yes

Part 3: Basic Configuration of Router R1

Step 1: Configure basic settings of Router R1.

a. Disable DNS lookup.

b. Configure the device name as shown in the topology.

c. Assign **class** as the privileged EXEC encrypted password.

d. Assign **cisco** as the console password, enable login

e. Configure **logging synchronous** to prevent console messages from interrupting.

f. Configure password encryption

g. Copy the running configuration to the startup configuration.

```
R1(config)# hostname R1
R1(config)# no ip domain-lookup
R1(config)# enable secret class
R1(config)# banner motd # Restricted Access. #

R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1# copy running-config startup-config
```

Part 4: Trunk-Based Inter-VLAN Routing at Router R1

Step 1: 802.1Q Trunk from Switch S1 to Router R1

a. Create a trunk on interface G0/1 of switch S1 and allow all VLANs 10,20, and 99 to be transmitted over the trunk.

```
S1(config)# interface g0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 10,20,99
```

Step 2: Router Interfaces for all VLANs.

a. For each VLAN in VLAN Table, create a sub-interface on R1 G0/0/0.ID, using the VLAN number as the sub-interface ID.

b. Finally, switch on the physical interface G0/0/0.

```
R1(config)# interface g0/0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config)# interface g0/0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0

R1(config)# interface g0/0/0.99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip address 192.168.99.1 255.255.255.0

R1(config)# interface g0/0/0
R1(config-if)#no shut
```

Step 3: Display Device Information

a. Issue the **show interfaces trunk** command to view the trunk mode on S1.

Record, which encapsulation is used on the trunk link at interface G0/1? 802.1q

Which VLANs are allowed on the trunk? 10,20,99

What is the native VLAN on your trunk? 1

b. List the subnets, which are routed at R1 (**show ip route**).

```
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0/0.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0/0.10
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0/0.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0/0.20
     192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.99.0/24 is directly connected, GigabitEthernet0/0/0.99
L       192.168.99.1/32 is directly connected, GigabitEthernet0/0/0.99
```

Step 4: Test Connectivity between VLANs

a. Check connectivity (ping) from PC1 to router R1 in VLAN 10. Connectivity (y/n)? y

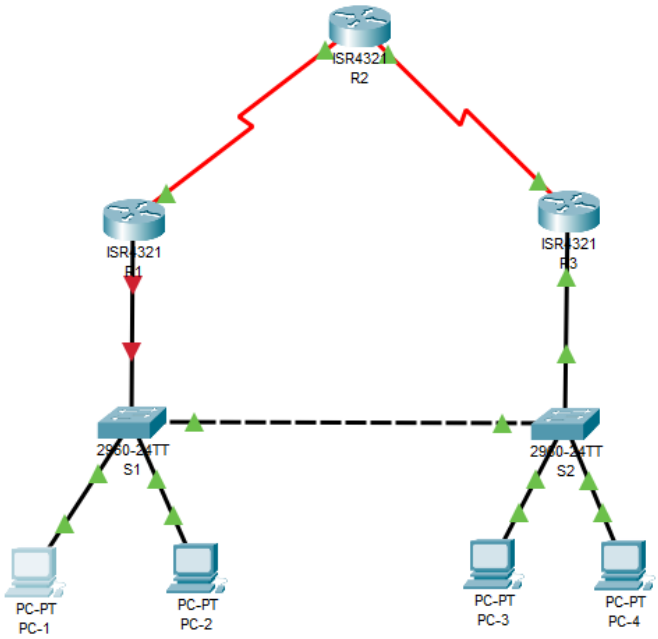
b. Check connectivity (ping) from PC1 to switch S1 in VLAN 99. Connectivity (y/n)? y

c. Check connectivity (ping) from PC1 to PC2 in VLAN 20. Connectivity (y/n)? y

Note: Remove errors, if checks are not working.

Task 2 – Switch LAN Security

Topology



Modified and Extended VLAN Table

Switch	VLAN Number	VLAN Name	Access Port Membership	Network
SW-1	10	Admin	Fa0/2	192.168.10.0/24
	20	Sales	Fa0/3	192.168.20.0/24
	99	Management	Fa0/24	192.168.99.0/24
	100	NativeVLAN	Unused	None
	999	BlackHole	All unused	None
SW-2	10	Admin	Fa0/2	192.168.10.0/24
	20	Sales	Fa0/3	192.168.20.0/24
	99	Management	Fa0/24	192.168.99.0/24
	100	NativeVLAN	Unused	None
	999	BlackHole	All unused	None

Part 1: Switch Port Security

Step 1: Create all VLANs

a. Extend the VLAN database with all VLANs of the Modified and Extended VLAN table.

b. Create VLAN 100 and give it the name NativeVLAN on both switches.

c. Create VLAN 999 and give it the name BlackHole on both switches.

```
S1(config)# vlan 100
S1(config-vlan)# name NativeVLAN
S1(config)# vlan 999
S1(config-vlan)# name BlackHole
```

Step 2: New Access Ports for VLAN 99

a. Configure switch ports F0/24 of both switches S1 and S2 as access port to VLAN 99.

```
S1(config)# int f0/24
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
```

Step 3: Create Secure Trunks

Recognize that interface Fa0/1 and G0/1 of both switches S1 and S2 are no longer access port, but will become trunk ports.

a. Interface Fa0/1 on both switches and Interface G0/1 on switch S2 shall be static trunks now.

1. Remove F0/1 access port allocation (no switchport access vlan 10)
2. Configure port Fa0/1 and G0/1 as static trunks.
3. Allow only given VLANs on trunk.
4. For all trunk interfaces on both switches **disable DTP negotiation**.
5. Configure all trunk ports on both switches to use VLAN 100 as the native VLAN.

```
S1(config)#int f0/1
S1(config-if)#no switchport access vlan 10
S1(config-if)#end
S1(config)#int f0/1
S1(config-if)# switchport mode trunk
S1(config)#int g0/1
S1(config-if)# switchport mode trunk
S1(config-if)#switchport trunk allowed vlan10
S1(config-if)#switchport trunk allowed add vlan20
S1(config-if)#switchport trunk allowed add vlan99
S1(config)#int f0/1
S1(config-if)#switchport nonegotiate
S1(config)#int f0/1
S1(config-if)#switchport trunk native vlan 100
```

b. Change and extend configuration of interface G0/1 of switch S1 accordingly.

Step 4: Secure Unused Switchports at switch S1.

a. Shutdown all unused switch ports on S1.

b. Move all unused switch ports to the BlackHole VLAN.

```
S1(config)#interface range fastEthernet 0/4-23,int g0/2
S1 (config-if-range)#shutdown
S1(config)#interface range fastEthernet 0/4-23,int g0/2
S1 (config-if-range)#switchport access vlan 999
```

c. List your VLAN database on **S1** (**show vlan brief**).

Record, which switch ports are in VLAN 1 now:

There is no port in VLAN 1

```
S1#show vlan brief
VLAN Name                         Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                      active
10   Admin                         active    Fa0/2
20   Sales                        active    Fa0/3
99   Management                        active    Fa0/24
100  NativeVLAN                        active
999  BlackHole                    active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                  Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                  Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                  Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                  Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                  Gig0/2
1002 fddi-default                 active
1003 token-ring-default                active
1004 fddinet-default               active
1005 trnet-default                active
```

Step 5: Port Security at switch S1.

a. Activate port security on all active access ports on switch S1.

```
S1(config)#interface range f0/2-3,f0/24
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport port-security
```

b. Configure the active ports to allow a maximum of 4 MAC addresses to be learned.

```
S1(config)#int range f0/2-3, f0/24
S1(config-if-range)#switchport port-security maximum 4
```

c. For port F0/2 on S1, statically configure the MAC address of the PC using port security.

```
S1(config)#int f0/2
S1(config-if)#switchport port-security mac-address 00D0.97B4.6B0E:20
```

d. Configure each active access port, that it will automatically add the MAC addresses learned on the port to the running configuration.

```
S1(config)#int range f0/2-3, f0/24
S1(config-if-range)#switchport port-security mac-address sticky
```

e. Configure the port security violation mode to drop packets from MAC addresses that exceed the maximum, generate a Syslog entry, but do not disable the ports.

```
S1(config)#int range f0/2-3, f0/24
S1(config-if-range)#switchport port-security violation restrict
```

f. From PC2, ping router R1. Check Port Security Options at S1 interface F0/3 (**show port-security interface f0/3**).

If available, record the MAC address of PC2: 00D0.97B4.6B0E:20

Part 2: STP and DHCP Security

Step 1: STP security with PortFast, and BPDU Guard.

g. On switch S1

1) Enable PortFast on all the access ports that are in use.

2) Enable BPDU Guard on all the access ports that are in use.

```
S1(config)#int range f0/2-3, f0/24
S1(config-if-range)#spanning-tree portfast
S1(config-if-range)#spanning-tree bpduguard enable
```

Step 2: DHCP Snooping.

For exercise purposes, we configure DHCP snooping, although DHCP is not use in this Lab.

h. On switch S1

1) Configure the trunk ports on S1 as trusted ports.

2) Limit the untrusted ports on S1 to five DHCP packets per second.

```
S1(config)#interface range f0/1, g0/1
S1(config-if-range)#ip dhcp snooping trust
```

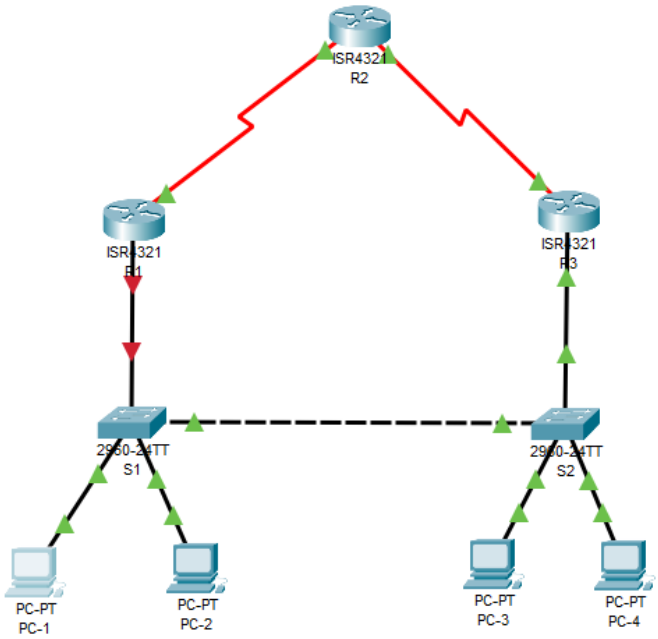
```
S1(config)#interface range f0/2-3,f0/24
S1(config-if-range)#ip dhcp snooping limit rate 5
```

i. On switch S2, enable DHCP snooping globally and for VLANs 10, 20 and 99.

```
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping vlan 10,20,99
```

Task 3 – Static Routing

Topology



Extended Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/0.10	192.168.10.1	255.255.255.0	N/A
	G0/0/0.20	192.168.20.1	255.255.255.0	N/A
	G0/0/0.99	192.168.99.1	255.255.255.0	N/A
	S0/1/0 (~~DCE~~) DTE	10.1.1.1	255.255.255.252	N/A
R2	S0/1/0	10.1.1.2	255.255.255.252	N/A
	S0/1/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo1 (loopback)	209.165.200.225	255.255.255.224	N/A
R3	G0/0/0.10	192.168.10.3	255.255.255.0	N/A
	G0/0/0.20	192.168.20.3	255.255.255.0	N/A
	~~S0/0/1~~ S0/1/0	10.2.2.1	255.255.255.252	N/A
S1	VLAN99	192.168.99.101	255.255.255.0	192.168.99.1
S2	VLAN99	192.168.99.102	255.255.255.0	192.168.99.1
PC-1	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC-3	NIC	192.168.10.33	255.255.255.0	192.168.10.3
PC-2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC-4	NIC	192.168.20.24	255.255.255.0	192.168.20.3

Part 3: Basic Router Configuration

Step 1: Configure basic settings for router R2 and R3.

a. Disable DNS lookup.

b. Configure device name

c. Assign **class** as the privileged EXEC encrypted password.

d. Assign **cisco** as the console password, enable login

e. Configure **logging synchronous** to prevent console messages from interrupting.

f. Configure password encryption

g. Save your running configuration in the startup configuration.

```
R1(config)# hostname R2
R1(config)# no ip domain-lookup
R1(config)# enable secret class
R1(config)# banner motd # Restricted Access. #

R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1# copy running-config startup-config
```

Step 2: Configure G0/0/0 interface of router R3

a. Configure all sub-interfaces of router R3 as listed in the Addressing Table.

b. Switch-on interface G0/0/0.

```
R3(config)#int g0/0/0.10
R3(config-subif)#encapsulation dot1Q 10
R3(config-subif)#ip add 192.168.10.3 255.255.255.0
R3(config-subif)#exit

R3(config)#int g0/0/0
R3(config-subif)#no shut
```

Step 3: Configure serial interface at all routers

a. Configure all serial interfaces at router R1, R2, and R3 as listed in the Addressing Table.

b. Set clock rate to **125000** (125 kHz) for all DCE serial interfaces.

Check interface type (DCE/DTE) (**show controller <serial interface>**)

c. Switch on serial interfaces

d. Copy the running configuration to the startup configuration.

```
R1# configure terminal
R1(config)# interface s0/1/0
R1(config-if)# clock rate 125000

R1(config)# interface serial 0/1/0
R1(config-if)# ip address 10.1.1.1 255.255.255.252

R2(config)# interface serial 0/1/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252

R2(config)# interface serial 0/1/1
R2(config-if)# ip address 10.2.2.2 255.255.255.252

R3(config)# interface serial 0/1/0
R3(config-if)# ip address 10.2.2.1 255.255.255.252
```

Step 4: Configure Loopback interface at router R2

a. Configure loopback interface Lo1 as listed in the Addressing Table.

b. Copy the running configuration to the startup configuration.

```
R3(config)# interface GigabitEthernet 0/0/0.10
R3(config-subif)# encapsulation dot1Q 10
R3(config-if)# ip address 192.168.10.3 255.255.255.0
R3(config)# interface GigabitEthernet 0/0/0.20
R3(config-subif)# encapsulation dot1Q 20
R3(config-if)# ip address 192.168.20.3 255.255.255.0

R2# configure terminal
R2(config)# interface loopback 1
R2(config-if)# ip address 209.165.200.225 255.255.255.224
R2(config-if)# exit
```

Step 5: Connectivity Check

a. Check connectivity (ping) from R2 to router R1 (serial interface). Connectivity (y/n)? y

b. Check connectivity (ping) from R2 to router R3 (serial interface). Connectivity (y/n)? y

Note: Remove errors, if checks are not working.

c. At router R2 inspect the routing table.

List the networks which are routed at R2:

```
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/1/0
L       10.1.1.2/32 is directly connected, Serial0/1/0
C       10.2.2.0/30 is directly connected, Serial0/1/1
L       10.2.2.2/32 is directly connected, Serial0/1/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/27 is directly connected, Loopback1
L       209.165.200.225/32 is directly connected, Loopback1
```

Which networks are missing in the routing table?

192.168.10.0/24
192.168.20.0/24

Part 4: Static Route Configuration

Step 1: Static Routing in router R1, and R3

Because there are remote networks for all routers, we must add routes in all routers.

a. In router R1, configure a static default route to exit the serial interface. R1(config)#ip route 0.0.0.0 0.0.0.0 serial 0/1/0

b. In router R3, configure a static default route to exit the serial interface. R3(config)#ip route 0.0.0.0 0.0.0.0 serial 0/1/0

Step 2: Static Routing in router R2

a. Configure a default route with exit to the loopback interface Lo1. R2(config)#ip route 0.0.0.0 0.0.0.0 Loopback1

b. Configure a static route to all VLAN networks 192.168.xx.0 / 24 with next hop R1.

R2(config)#ip route 192.168.10.0 255.255.255.0 10.1.1.1
R2(config)#ip route 192.168.20.0 255.255.255.0 10.1.1.1
R2(config)#ip route 192.168.99.0 255.255.255.0 10.1.1.1

Step 3: Verify connectivity.

a. From PC1, you should be able to ping the serial interface of router R1, Successful (y/n)? y

b. From PC1, you should be able to ping the loopback interface of router R2, Successful (y/n)? y

c. From PC4, you should be able to ping the loopback interface of router R2, Successful (y/n)? y

Note: Remove errors, if checks are not working.

Step 4: Review routing path

a. Traceroute from PC1 to the loopback interface of router R2.

List all interfaces to and from the loopback interface to record the routing path.

To: (from PC1 to R2-LB1): R1-int000.10, R2-S0/1/0, LB1
From: (from R2 to PC1): R1-S0/1/0, PC1

b. Traceroute from PC4 to the loopback interface of router R2.

List all interfaces to and from the loopback interface to record the routing path.

To (from PC4 to R2-LB1): R3-int000.20, R2-S0/1/1, LB1
From: (from R2 to PC1): R1-S0/1/0, PC1

Discuss, why the return path is different of the forwarding path.

This because of the static route provided in router R2 for destination 192.168.20.0/24 to R1's serial interface0/1/0's IP as next hop

Deliverables

Lab Teams

This lab may be solved in teams of max. 3 students. All teams have to provide their deliverables in time.

Teams are grouped into 2 groups, which have different due dates and presentation dates.

Module Group Exams

Each team member must solve the requested **Module Group Exams** before delivery date.

Deliverables

Each teams delivers the following documents and files:

- One **PDF-File (.pdf)** with the completed **Homework and Instructions**.
  All tasks and questions must be answered.
- One **PacketTracer-File** (.pka) in PacketTracer Version 8 with your **final configuration**.
- One **Text-File in** ASCII-Format (.txt, simple Text Editor) with the **running configurations of Router R1, and Switch S1**.