

CCNA

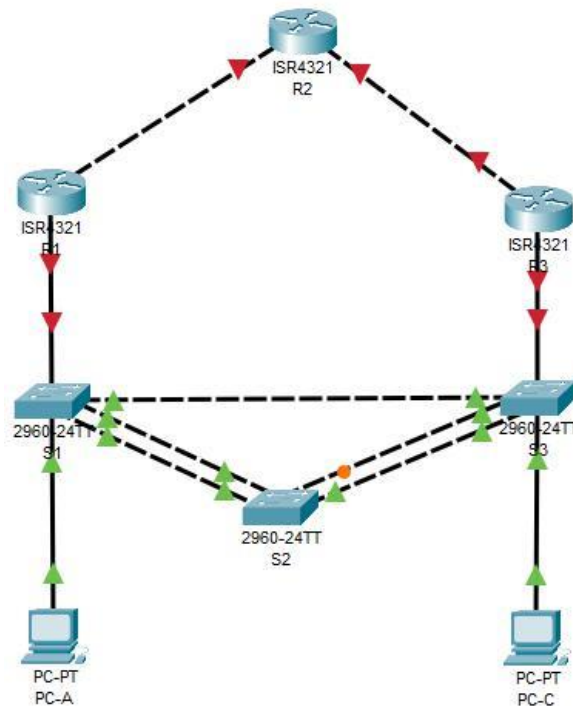
SRWE Lab 2

Names:

Team-No.: 04

Sanjida,Febin,Rubaiya

Spanning Tree Protocols EtherChannel, HSRP Redundancy



Lab Preparations

SRWE Assessments: Modules 5-6: Redundant Networks Exam
Modules 7-9: Available and Reliable Networks Exam

NP Course: NP Chapter 9

Cisco IOS Commands

Lab Instructions

Task 1 - Examine STP Protocols

Task 2 - LACP EtherChannel Link Aggregation

Task 3 - HSRP Default Gateway Redundancy

Deliverables and List of Due Dates

Write your answers in **red color**. You may use the comment capabilities of the free Adobe reader.

Preparation

Part 1: Cisco IOS Basic Configuration Commands

- Read the **Lab Instructions** of this Lab, and read NP chapter 9
- Check the **IOS Command List**, provided for the Labs and Review already used and new configuration commands.

Part 2: Cisco IOS PVST+ and Rapid PVST+

- What is the maximum default time for switch-over to redundant Ethernet links when using legacy IEEE 802.1D-1998 STP (PVST+)? **50s**

- Set a switch to primary root for VLAN 10.

```
S1(config)# spanning-tree vlan 10 root primary
```

- Enable Rapid PVST+ on a switch.

```
S1(config)# spanning-tree mode rapid-pvst
```

- Sets PortFast mode and BPDUGuard on access port f0/1?

```
S1(config)# int f0/1
```

```
S1(. .)# spanning-tree portfast
```

```
S1(. .)# spanning-tree bpduguard enable
```

Part 3: EtherChannel

- Which requirements must be fulfilled to form an EtherChannel?

A link aggregation technology is needed that permits redundant links between devices is known as EtherChannel. EtherChannel is a link aggregation technology that groups multiple physical Ethernet links together into one single logical link(ref) requirements:

same speed, same interface, same trunk configuration

- What could prevent successful EtherChannel configuration?

If requirements are not matched like if Interface types are mixed and the individual EtherChannel group member port configuration is not consistent on both devices

- Create an EtherChannel channel-group 2 (Po2), mode active, for the interface range f0/1 – f0/2.

```
S1(config)# interface range f0/1-f0/2
```

```
S1(. .)# channel-group 2 mode active (passive)
```

- d. Configure the EtherChannel interface port-channel 2 (Po2) as trunk, with Native VLAN 99, and allowed VLANs are 1, 100, 99.

```
S1 (config) # interface range f0/1-f0/2
S1 (config-if) # interface port-channel 2
S1 (config-if) # switchport mode trunk
S1 (config-if) # switchport trunk native vlan 99
S1 (config-if) # switchport trunk allowed vlan 1,100,99
S1 (config-if) # exit
```

Part 4: FHRP and HSRP

- a. What makes it that critical, not to use only one router for the default gateway operation in a network?

A mechanism is needed to provide alternate default gateways in switched networks where two or more routers are connected to the same VLANs. That mechanism is provided by first hop redundancy protocols (FHRPs). In a switched network, each client receives only one default gateway. There is no way to use a secondary gateway, even if a second path exists to carry packets off the local segment. For example, if R1 is responsible for routing packets from PC1 and If R1 becomes unavailable, the routing protocols can dynamically converge to R2. R2 now routes packets from outside networks that would have gone through R1. (ref)

- b. Describe the following functions in

(references)

Virtual Router: A wireless router implemented in software in a computer with wired Internet access and Wi-Fi capability.

Virtual IP address: A virtual IP address (VIP or VIPA) is an IP address that doesn't correspond to an actual physical network interface.

Virtual MAC address: The Virtual MAC address allows the High Availability pair to share the same MAC address, which dramatically reduces convergence time following a failover.

Active Router: The Active router is responsible for forwarding the traffic. If it fails, the Standby router takes up all the responsibilities of the active router and forwards the traffic.

Standby Router: The Standby router takes up all the responsibilities of the active router and forwards the traffic.

- c. Create a virtual router with HSRP on router R1 (interface g0/1) and R2 (interface f0/3). Virtual IP address is 172.16.10.200 / 24. R1 is active router with priority 150. R2 is passive router.

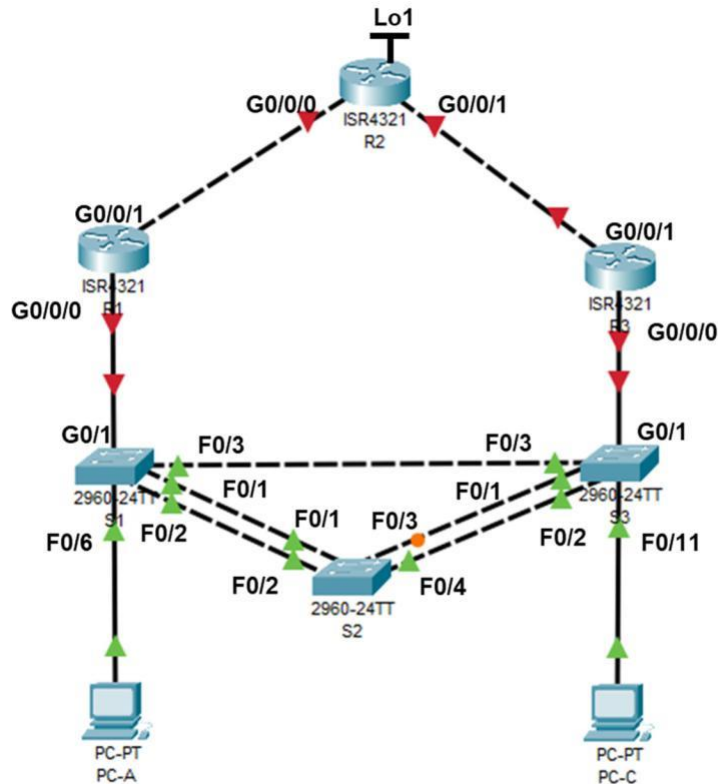
```
R1 (config) # int g0/1
R1 (config-if) # standby 1 ip 172.16.10.200
R1 (config-if) # standby 1 priority 150
R1 (config-if) # standby 1 preempt
R2 (config) # int g0/3
R2 (config-if) # standby 1 ip 172.16.10.200
```

- d. What is the difference of HSRP and GLBP?

The main difference is that GLBP allows the load balancing of traffic among the master and standby routers while in HSRP (and VRRP) the standby routers do not help handle traffic. With GLBP, the single virtual IP address is associated with one virtual MAC address per GLBP member. (ref)

Task 1 – Examine STP Protocols

Packet Tracer Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/0	192.168.10.1	255.255.255.0	N/A
	G0/0/1	10.1.1.1	255.255.255.252	N/A
R2	G0/0/0	10.1.1.2	255.255.255.252	N/A
	G0/0/1	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	192.168.10.3	255.255.255.0	N/A
	G0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 99	192.168.99.11	255.255.255.0	192.168.99.1
S2	VLAN 99	192.168.99.12	255.255.255.0	192.168.99.1
S3	VLAN 99	192.168.99.13	255.255.255.0	192.168.99.1
PC-A	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.10.33	255.255.255.0	192.168.10.3 (!)



VLAN Assignments

VLAN	Name
10	User
99	Management

Part 1: Set Up Network Topology and Initialize Devices

Step 1: Build topology in Packet Tracer.

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

- Build the network with ISR4321 router, 2960 switches, and PCs in Packet Tracer. Rename the devices.
- Cable the network according to the topology with straight-through TP cables  and cross-over cables .
- We will use the CLI window of the network devices directly for configurations.
- Configure IP address, net mask and default gateway for PC-A, and PC-C.

Step 2: Configure some basic settings for switches S1, S2 and S3.

Double-click network devices and use the CLI window. When network device is booting up, skip any automatic configuration.

For Switch S1, S2, and S3, perform the following tasks:

- Disable DNS lookup.
- Configure device name
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password, enable login, configure **logging synchronous** to prevent console messages from interrupting.
- Configure password encryption
- Save your running configuration in the startup configuration.

Part 2: Configure VLANs and Trunks

Step 1: VLANs and Access Ports

- Create** VLAN 10 (name User) and VLAN 99 (name Management) on all of the switches.
- Configure **access ports** with VLAN 10:
-switch S1 port F0/6 and switch S3 port F0/11

Step 2: Trunk ports and native VLAN 99.

- For all ports interconnecting switches, S1 (F0/1, F0/2, F0/3), S2 (F0/1, F0/2, F0/3, F0/4), S3 (F0/1, F0/2, F0/3) enable and configure trunk ports
 - assign native VLAN 99
 - allow all configured VLANs

Step 3: Management Interface SVI.

- a. Configure the SVI VLAN 99 and apply the IP addresses from Addressing Table on all switches.
- b. Add the Default Gateway 192.168.99.1 to all switches.

Step 4: Verify configurations and connectivity.

- a. Use the **show vlan brief** command on S1.

S1#sh vlan br

VLAN Name Status Ports

1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5
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, Fa0/24, Gig0/1, Gig0/2

10 User active Fa0/6
99 Management active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

S1#

Which Port is assigned to VLAN 10? Fa0/6

- b. Use the **show interfaces trunk** command on S2.
 - Which ports are trunk ports?

S2#

S2#sh int trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 99
Fa0/2 on 802.1q trunking 99
Fa0/3 on 802.1q trunking 99
Fa0/4 on 802.1q trunking 99

Port Vlans allowed on trunk

Fa0/1 1,10,99
Fa0/2 1,10,99
Fa0/3 1,10,99
Fa0/4 1,10,99

Port Vlans allowed and active in management domain

Fa0/1 1,10,99
Fa0/2 1,10,99
Fa0/3 1,10,99
Fa0/4 1,10,99

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,99

Fa0/2 1,10,99

Fa0/3 1,10,99

Fa0/4 none

- Which VLANs are allowed on all trunks? 1,10,99 Vlans allowed on trunk

c. Configure PC-A and PC-C.

By pinging, verify connectivity from PC-A to PC-C. Connectivity is given (y/n)? yes

Part 3: Set Root Bridge and Examine PVST+ Convergence

Step 1: Determine the current root bridge.

Note: There are three instances of the spanning tree on each switch. The default STP configuration on Cisco switches is PVST+, which creates a separate spanning tree instance for each VLAN (VLAN 1 and any user-configured VLANs).

Use the command **show spanning-tree** on all three switches to determine the answers to the following questions:

Record the bridge priority for **VLAN 10** in switch S1, S2, and S3:

S1 32778

S2 32778

S3 32778

Which switch is the root bridge for **VLAN10**? S3

Why was this switch elected as the root bridge for **VLAN10**? MAC address

Bridge ID Priority 32778 (priority 32768 sys-id-ext 10)

Address 0001.C91B.0641

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Step 2: Primary and secondary root bridge for all existing VLANs.

Having a root bridge (switch) elected by MAC address may lead to a suboptimal configuration. In this lab, you will configure switch S2 as the root bridge and S1 as the secondary root bridge.

- Configure switch S2 to be the **primary root bridge** for VLAN 10.
- Configure switch S1 to be the **secondary root bridge** for VLAN 10.
- Use the **show spanning-tree vlan 10** command to answer the following questions:

What is the bridge priority of S1 for VLAN 10 now? 28682

What is the bridge priority of S2 for VLAN 10 now? 24586

According to STP algorithm, which interfaces in the lab network should be blocked in the VLAN 10 spanning-tree (record switch name and interfaces, (Sx Fa0/y)): **S3 switch with Fa0/2, Fa0/3**

Check by **show spanning-tree vlan 10** which interfaces in the network are in blocking state in VLAN 10: **S3 switch with Fa0/2, Fa0/3**

Step 3: Change the Layer 2 topology and examine PVST+ convergence.

To examine PVST+ convergence, you will create a Layer 2 topology change.

- Record (**show spanning-tree vlan 10**) the state of interface F0/3 in VLAN 10 at switch S3: **na/blocked as blk**
- Create a topology change in VLAN 10 by disabling interface range **F0/1-2** on S3.

```
S3(config)#interface range f0/12
```

```
S3(config-if)#shutdown
```
- Name the port states of PVST+ (Per VLAN-STP), which interface **F0/3** should walk through during network convergence: **listening / learning / forwarding**

Record (**show spanning-tree vlan 10**) the state of interface F0/3 in VLAN 10 at switch S3 again: **Forwarding /FWD**

Interface Role Sts Cost Prio.Nbr Type

Fa0/3 Root FWD 19 128.3 P2p
Fa0/11 Desg FWD 19 128.11 P2p

- (Skipped) In non-COVID-19 times, you would use debugging of spanning-tree (**S3#debug spanning-tree**) to record the convergence time with real switches.

Using the time stamp from the first and last STP debug message, calculate the time in seconds that it took for the network to converge. **Hint:** The debug timestamp format is **date hh.mm.ss:msec**.

Result: ~ 30 sec.

Part 4: Rapid PVST+ plus PortFast and BPDUGuard

Step 1: Rapid PVST+.

- Configure all switches S1, S2, and S3, for using Rapid PVST+.

Step 2: Examine Rapid PVST+ convergence.

- (Must do) Create a topology change by enabling interface range **F0/1-2** on S3 again.

```
S3(config)#interface range f0/12
```

```
S3(config-if)#no shutdown
```


- b. **(Skipped)** you would use debugging of spanning-tree (**S3#debug spanning-tree**) to record the convergence time with real switches.

After all messages of the topology change have been received stop debug mode by the command **no debug spanning-tree events**.

Using the time stamp from the first and last Rapid RSTP debug message, calculate the time that it took for the network to converge.

Result: < 1ms

Step 3: PortFast and BPDUGuard

PortFast is a feature of spanning tree that transitions a port immediately to a forwarding state as soon as it is turned on. This is useful in connecting hosts so that they can start communicating on the VLAN instantly, rather than waiting on spanning tree.

BPDUGuard prevents form STP attack from access ports

- a. Configure all access ports on switch S1 and S3 with PortFast mode.

spanning-tree portfast

In which state are switch ports, which have been configured with PortFast?

forwarding

Fa0/6 Desg FWD 19 128.6 P2p

- b. Configure all access ports on switch S1 and S3 to be protected against STP attacks.

spanning-tree bpduguard enable

Record the status of Port F0/11 at switch S3:

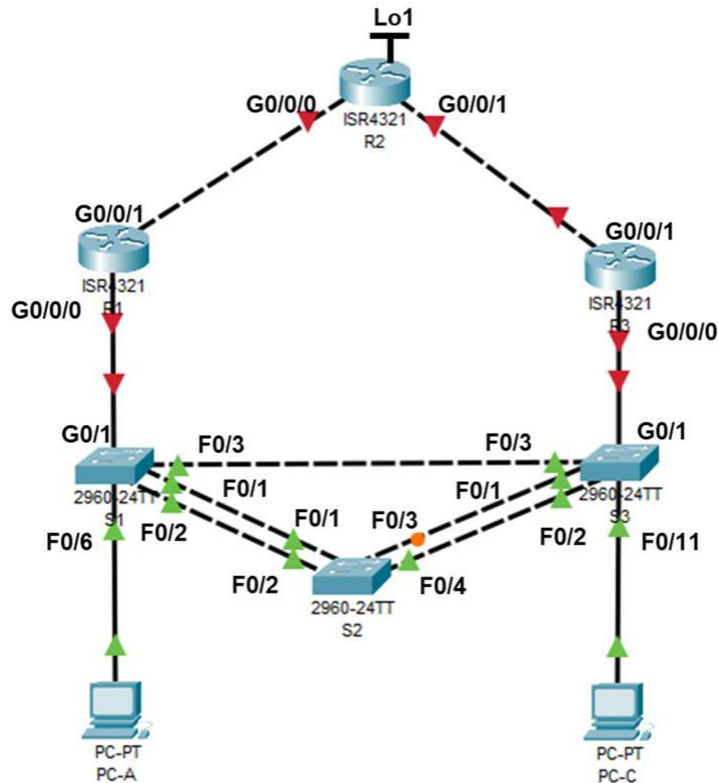
forwarding

Reflections

- a. What is the main benefit of using Rapid PVST+?
allows faster spanning-tree calculations and convergence in response and provides optimized performance (ref)
- b. How does configuring a port with PortFast allow for faster convergence?
permits for an access port to transit into a learning, discarding, forwarding status which minimizes convergence time.
- c. Any idea how BPDU guard prevents from STP initiated denial-of-service (DOS) attacks?
If a port is BPDU guard enabled and it gets BPDU frames from outside, then the access port gets disabled. Also violation of policy is reported and gets stopped in such a way. (ref)

Task 2 - LACP EtherChannel Link Aggregation

Packet Tracer Topology



We continue with the PT Topology and Addressing Table.

Part 1: Configure Link Aggregation Control Protocol (LACP)

LACP is a link aggregation protocol developed by the IEEE. In this Part, the link between S1 and S2, and the link between S2 and S3 will be configured using LACP.

Step 1: Configure LACP between S1 and S2.

- Configure the link between S1 and S2 as channel-group 2 (Po2)
 - Use LACP as the link aggregation protocol.
 - Switch S1 shall get EtherChannel mode **active**, switch S2 EtherChannel shall get EtherChannel mode **passive**.
- Configure channel-groups to be trunk ports with the same trunk conditions of Task 1.
- Verify that the ports have been aggregated. Use **show etherchannel summary**.
 - What protocol is Po2 using for link aggregation? **LACP**

Group	Port-channel	Protocol	Ports
2	Po2(SU)	LACP	Fa0/1(P) Fa0/2(P)

- Which interface name is given to the aggregated link? **Po2(SU)**
- Which state information (flags) are given for this interface? **SU, S=LAYER 2, U= IN USE**
- How many channel groups are in use? **ONE**

Step 2: Verify that the ports are configured as trunk ports.

- Issue the **show interfaces trunk** command on S1.
- Check trunk ports and native VLAN.

Trunk ports on S1? **Po2, Fa0/3**

S1#sh int trunk

Port	Mode	Encapsulation	Status	Native vlan
Po2	on	802.1q	trunking	99
Fa0/3	on	802.1q	trunking	99

Native VLAN on trunk ports on S1? **99**

In case of native VLAN mismatch, correct native VLAN on the aggregated channel group PO2.

- From the **show spanning-tree** output, record port cost and port priority of the aggregated link Po2.
Po2 cost> 9 , priority> 128.28

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Fa0/3	Desg	FWD	19	128.3		P2p
Po2	Altn	FWD	9	128.28		Shr

Step 3: Configure LACP between S2 and S3.

- Similar to Po2, configure the links between S2 and S3 as channel-group Po3 and use LACP as the link aggregation protocol.
Name the LACP interface between S2 and S3 **channel-group 3**
(Po3) Po3 at S2 is in LACP mode active.
- Verify that the EtherChannel has formed by **show etherchannel summary**. EtherChannel is active (y/n)? **yes**

Step 4: Verify end-to-end connectivity.

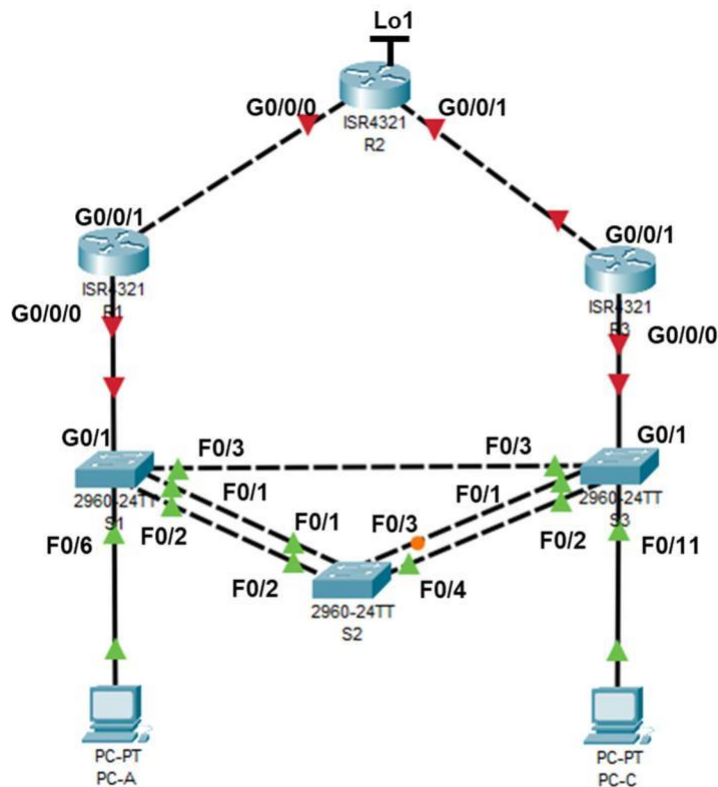
Verify that devices can ping each other within the same VLAN. If not, troubleshoot until there is end-to-end connectivity.

From S3 ping S1 and S2. Ping works (y/n)? **yes**

From PC-A ping PC-C. Ping works (y/n)? **yes**

Task3 – HSRP Default Gateway Redundancy

Packet Tracer Topology



We continue with the PT Topology and Addressing Table.

Background / Scenario

First Hop Redundancy Protocols (FHRPs) provide redundant default gateways for end devices with no end-user configuration necessary.

Part 1: Extent Switch Configuration

Step 1: Configure Additional Access Ports for VLAN 10

For simplification, we only route the network of VLAN 10 (192.168.10.0 / 24) and allocate all switch ports to routers as access ports in VLAN 10.

(An alternative option is to configure router-on-a-stick.)

- On switch S1, configure interface G0/1 as Access Port for VLAN 10. **done**
- On switch S3, configure interface G0/1 as Access Port for VLAN 10. **done**

Part 2: Basic Router Configuration

Step 1: Configure basic settings for each router.

- 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, configure **logging synchronous** to prevent console messages from interrupting.
- e. Configure password encryption
- f. Save your running configuration in the startup configuration.

Step 2: Router Interfaces

- a. Configure IP addresses for the router interfaces (R1, R2 and R3) as listed in the Addressing Table.
- b. In router R2 also create a loopback interface Lo1 with IP address 209.165.200.225 and mask 255.255.255.224, which simulates Internet access.

Step 3: Static Routing

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 interface G0/0/1.
- b. In router R2, configure a static route to network 192.168.10.0 / 24 with exit interface G0/0/1.
- c. In router R2, configure a default route with exit to the loopback interface Lo1.
- d. In router R3, configure a static default route to exit interface G0/0/1.

Step 4: Verify connectivity.

- a. From PC-A, you should be able the default gateway at R1 (y/n). **yes**
- b. From PC-C, you should be able the default gateway at R3 (y/n). **yes**
- c. From PC-C, you should be able to ping the G0/0/1 interface at R2 (y/n). **yes**
- d. From PC-C, you should be able to ping the Lo1 loopback interface at R2 (y/n). **yes**

Part 3: First Hop Redundancy with HSRP

Even though the topology has been designed with some redundancy (two routers and two switches on the same LAN network), both PC-A and PC-C are configured with only one gateway address. If the R3 router or the interfaces on the router went down, PC-C could lose its connection to the Internet.

Step 1: Determine the path for Internet traffic for PC-A and PC-C.

From a command prompt on PC-A, issue a **tracert** command to the 209.165.200.225 loopback address of R2. Which path did the packets take from PC-A? **PC-A>R1>R2**

C:\>tracert 209.165.200.225

Tracing route to 209.165.200.225 over a maximum of 30 hops:

1 75 ms 0 ms 0 ms 192.168.10.1

2 * * * Request timed out.

3 14 ms 13 ms 50 ms 209.165.200.225

Trace complete.

From a command prompt on PC-C, issue a **tracert** command to the 209.165.200.225 loopback address of R2. Which path did the packets take from PC-C? **PC-C>R3>R2**

Step 2: Observe ICMP responses while breaking the link to the default router

- a. From a command prompt on PC-A, issue a **ping -t** command to the **209.165.200.225** address on R2. Make sure you leave the command prompt window open.
- b. As the ping continues, shut down the switch S1 interface G0/1. What happened to the ping traffic? It can't communicate anymore up to R2

Reply from 209.165.200.225: bytes=32 time<1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=15ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=11ms TTL=254
Request timed out.
Request timed out.

- c. Switch-on the switch S1 interface G0/1 again.
Re-issue a ping to 209.165.200.225 from PC-A to make sure connectivity is re-established. Is ping working again? **yes connection is regained.**

Step 3: HSRP on R1 and R3.

We use the virtual IP address **192.168.10.254** for HSRP.

R1 becomes the **active router** via configuration of the HSRP priority command with preemptive priority.
R3 is standby router.

- a. Configure HSRP on R1.
- b. Configure HSRP on R3.
- c. Verify HSRP by issuing the **show standby** command on R1 and R3.

Which priority has the active router? **Priority 150**

(configured150)

Which priority has the standby router? **Priority 100 (default 100)**

What is the MAC address for the virtual IP address? **0000.0C07.AC01**

- d. Use the **show standby** command on R1 and R3 to view an HSRP status summary.
At router R1 use **show standby brief** as well. Which information is missing compared to show standby?
state change, Mac addresses, hold time, preemptive enabled or not, group name

- e. Change the default gateway address at PC-A, and PC-C. Which address should you use?
Verify the new settings. Issue a ping from both PC-A and PC-C to the loopback address of R2. Are the pings successful (y/n)? **yess**

Step 4: Observe ICMP responses while breaking the link to the default router

- a. From PC-A use **tracert** to the Lo1 interface address 209.165.200.225. Record the path taken by the ICMP packets now. **PC-A>R1>R2**
- b. From PC-A issue a **ping -t** command to the **209.165.200.225** address on R2. Make sure you leave the command prompt window open.
As the ping continues, shut down the switch S1 interface G0/1. What happens to the ping traffic?
connection was not established first time for some seconds, the it re-established
How long was it interrupted? **approx. 9 sec**
- b. At PC-A stop ping (ctrl-c) and use **tracert** to the Lo1 interface address 209.165.200.225. Which path is taken now by the ICMP packets? **PC-A>R3>R2**
- c. Switch-on the switch S1 interface G0/1 again.
Re-issue **tracert** to 209.165.200.225 from PC-A to make sure connectivity to active router is re-established. **PC-A>R1>R2**
(Repeat tracert, if the path has not been changed yet.)

Deliverables

Lab Teams

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

Module Group Exams

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

Deliverables

Each teams uploads the following files:

- Create a PDF file **SRWE-Lab2-Result.pdf** with the completed and answered **Lab Preparations and Lab Instructions**.
All tasks must be worked on and all questions must be answered.
Write your answers in **red color**. You may use the comment capabilities of the free Adobe reader.
- Save your final Packet Tracer file **SRWE-Lab2-PT.pkt**
- Record the running configuration of switch S1 and both routers R1 and R2 (show run) in one text file **SRWE-Lab2-S1-R1-R2.txt**

Due Dates

Group 1	Teams 1-9	Due Date
	Module Group Exams 5-6, 7-9	17.01. – EOB
	Upload Deliverables	17.01. – EOB
	CCNA ZOOM Presentation	19.01. - 16:45 ff.

Group 2	Teams 1-9	Due Date
	Module Group Exams 5-6, 7-9	24.01. - EOB
	Upload Deliverables	24.01. - EOB
	CCNA ZOOM Presentation	26.01. - 16:45 ff.

- Per team you load one solution in Ilias in time.
- Per team you book one timeslot for acceptance.