CCNA SRWE   **Lab 2**   **Instruction**   **Deadline: 12.2.2021**
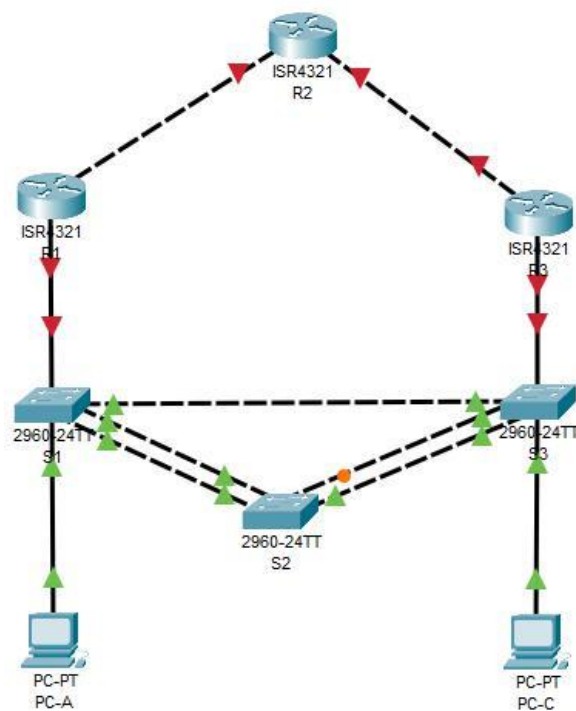
Name: Shabnaz Khanam

Spanning Tree Protocols

EtherChannel

HSRP Redundancy

NP Course   NP Chapter 9
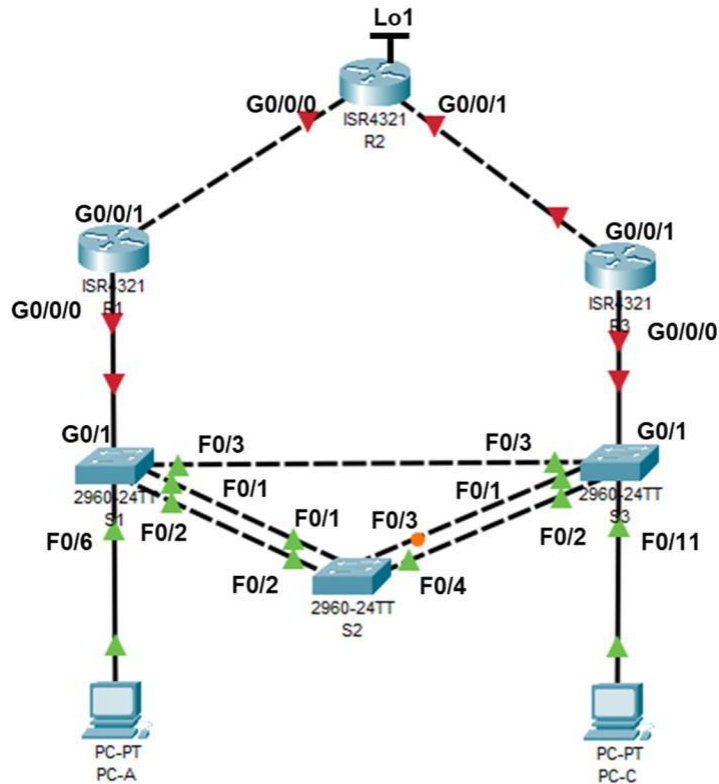
SRWE Modules 5 - 9:

Redundant Networks Exam

Available and Reliable Networks Exam

Answers and Solutions

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

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:

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 ⟋.

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

d.   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:

a.   Disable DNS lookup.

b.   Configure device name

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

a)   Assign **cisco** as the console password, enable login, configure **logging synchronous** to prevent console messages from interrupting.

d.   Configure password encryption

e.   Save your running configuration in the startup configuration.

Part 2:   Configure VLANs and Trunks

Step 1:   VLANs and Access Ports

a.   **Create** VLAN 10 (name User) and VLAN 99 (name Management) on all of the switches.

b.   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.

a.   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. Which Port is assigned to VLAN 10? Fa0/6

b. Use the **show interfaces trunk** command on S2.

   -   Which ports are trunk ports? fa0/1-4

   -   Which VLANs are allowed on all trunks? fa0/1-4

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

S2   Priority   32778 (priority 32768 sys-id-ext 10)

S3   Priority   32778 (priority 32768 sys-id-ext 10)

Which switch is the root bridge for **VLAN10**? S2

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

The default value is 32768, and the lowest number is preferred. In the case of a tie, the switch -2 with the lowest MAC address is selected.

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.

a. Configure switch S2 to be the **primary root bridge** for VLAN 10.

b. Configure switch S1 to be the **secondary root bridge** for VLAN 10.

c. Use the **show spanning-tree vlan 10** command to answer the following questions:

   What is the bridge priority of S1 for VLAN 10 now? Priority   28682 (priority 28672 sys-id-ext 10)

   What is the bridge priority of S2 for VLAN 10 now? Priority   24586 (priority 24576 sys-id-ext 10)

   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)):

   S1 FastEthernet0/1

   Check by **show spanning-tree vlan 10** which interfaces in the network are in blocking state in VLAN 10:   FastEthernet0/1

Page 4 of 12

NP	Networks and Protocols (NP)	Prof. Dr. A. Grebe

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

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

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

```
Physical     Config     CLI     Attributes

                        IOS Command Line Interface

Password:

s3>enable
Password:
s3#
s3#show spanningtree vlan 10
               ^
% Invalid input detected at '^' marker.

s3#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     000A.41A9.DB08
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00E0.B091.1EBC
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p

s3#
```

b.   Create a topology change in VLAN 10 by disabling interface range **F0/1-2** on S3.

S3(config)#**interface range f0/1-2**

S3(config-if)#**shutdown**

c.   Name the port states of PVST+ (Per VLAN-STP), which interface **F0/3** should walk through during network convergence:

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

```
Physical     Config     CLI     Attributes

                        IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

s3(config-if-range)#end
s3#
%SYS-5-CONFIG_I: Configured from console by console

s3#
s3#show spanningtree vlan 10
               ^
% Invalid input detected at '^' marker.

s3#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     000A.41A9.DB08
              Cost        38
              Port        3(FastEthernet0/3)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00E0.B091.1EBC
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/11           Desg FWD 19        128.11   P2p
Fa0/3            Root FWD 19        128.3    P2p
```

d.   (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+.

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

Step 2:   Examine Rapid PVST+ convergence.

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

```
S3(config)#interface range f0/1-2
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 <u>access</u> ports on switch S1 and S3 with PortFast mode.

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

b.   Configure all <u>access</u> ports on switch S1 and S3 to be protected against STP attacks.

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

```
s3#show interface status
Port        Name            Status       Vlan      Duplex  Speed Type
Po3                         connected    1         auto    auto
Fa0/1                       connected    1         auto    auto  10/100BaseTX
Fa0/2                       connected    1         auto    auto  10/100BaseTX
Fa0/3                       connected    1         auto    auto  10/100BaseTX
Fa0/4                       notconnect   1         auto    auto  10/100BaseTX
Fa0/5                       notconnect   1         auto    auto  10/100BaseTX
Fa0/6                       notconnect   1         auto    auto  10/100BaseTX
Fa0/7                       notconnect   1         auto    auto  10/100BaseTX
Fa0/8                       notconnect   1         auto    auto  10/100BaseTX
Fa0/9                       notconnect   1         auto    auto  10/100BaseTX
Fa0/10                      notconnect   1         auto    auto  10/100BaseTX
Fa0/11                      connected    10        auto    auto  10/100BaseTX
Fa0/12                      notconnect   1         auto    auto  10/100BaseTX
Fa0/13                      notconnect   1         auto    auto  10/100BaseTX
Fa0/14                      notconnect   1         auto    auto  10/100BaseTX
Fa0/15                      notconnect   1         auto    auto  10/100BaseTX
Fa0/16                      notconnect   1         auto    auto  10/100BaseTX
Fa0/17                      notconnect   1         auto    auto  10/100BaseTX
Fa0/18                      notconnect   1         auto    auto  10/100BaseTX
Fa0/19                      notconnect   1         auto    auto  10/100BaseTX
Fa0/20                      notconnect   1         auto    auto  10/100BaseTX
Fa0/21                      notconnect   1         auto    auto  10/100BaseTX
Fa0/22                      notconnect   1         auto    auto  10/100BaseTX
Fa0/23                      notconnect   1         auto    auto  10/100BaseTX
Fa0/24                      notconnect   1         auto    auto  10/100BaseTX
Gig0/1                      connected    10        auto    auto  10/100BaseTX
Gig0/2                      notconnect   1         auto    auto  10/100BaseTX

s3#
s3#|
```

Reflections

a. What is the main in benefit of using Rapid PVST+?

Rapid PVST+ decreases the time of Layer 2 convergence significantly over PVST+

b. How does configuring a port with PortFast allow for faster convergence?

PortFast allows for an access port to immediately transition into a forwarding state which decreases Layer 2 convergence time.

c. Any idea how BPDU guard prevents from STP initiated denial-of-service (DOS) attacks?

BPDU guard protects the STP domain by disabling access ports that receive a BPDU. BPDUs can be used in a denial of service attack that changes a domain's root bridge and forces an STP recalculation.

Task 2 - LACP EtherChannel Link Aggregation

Packet Tracer Topology
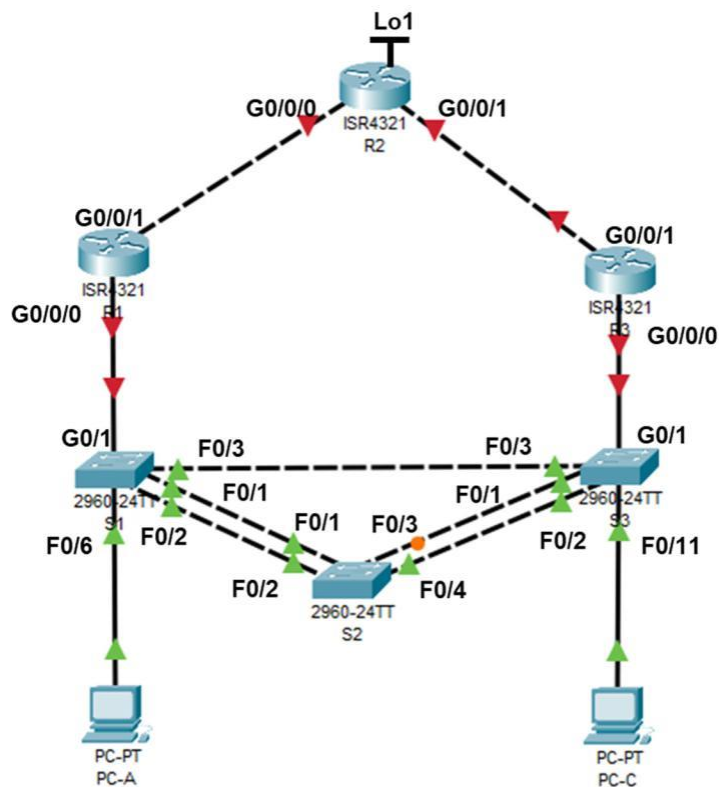
We continue with the PT Topology and Addressing Table.

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.

a. 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 shalle get EtherChannel mode **passive**.

b. Configure channel-groups to be trunk ports with the same trunk conditions of Task 1.

c. Verify that the ports have been aggregated. Use **show etherchannel summary**.

- What protocol is Po2 using for link aggregation?LACP

- Which interface name is given to the aggregated link? fa0/1-2

- Which state information (flags) are given for this interface? P

- How many channel groups are in use? 2

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

   a. Issue the **show interfaces trunk** command on S1.

   b. Check trunk ports and native VLAN.

   Trunk ports on S1? Fa0/3,Po2

   Native VLAN on trunk ports on S1? vlan 99

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

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

Step 3: Configure LACP between S2 and S3.

   a. 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.

   b. Verify that the EtherChannel has formed by **show etherchannel**

   summary. EtherChannel is active (y/n)?yes

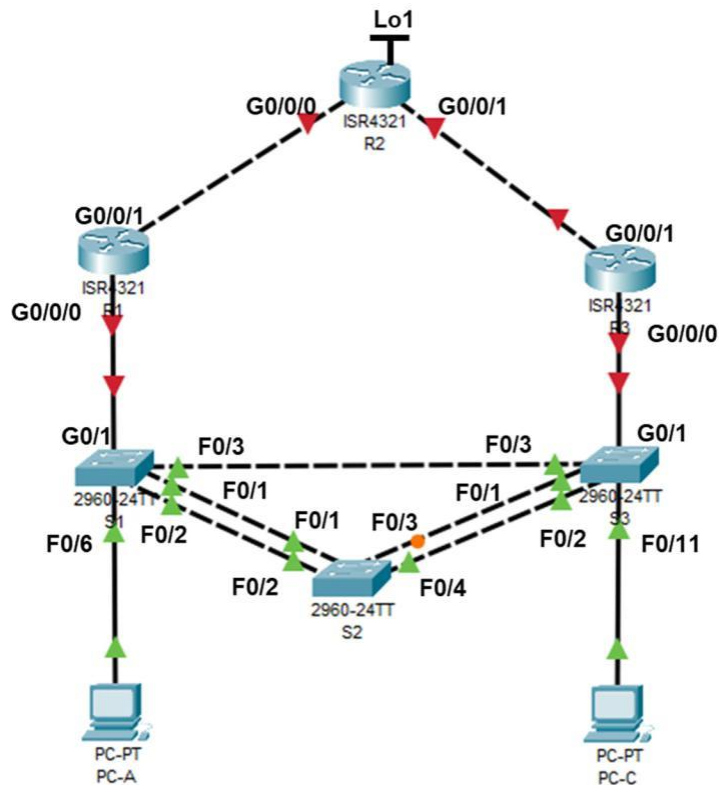### Step 4: Verify end-to-end connectivity.

   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

Lab 3 – 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.)

a.   On switch S1, configure interface G0/1 as Access Port for VLAN 10.

b.   On switch S3, configure interface G0/1 as Access Port for VLAN 10.

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.

a. 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?

   192.168.10.1 R1 intg0/0/0

b. 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?

   192.168.10.3 R3 int g0/0/0

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? Host is not reachable

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

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?R1

Which priority has the standby router?R3

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?
 Mac address

e. Change the default gateway address at PC-A, and PC-C. Which address should you use?

209.165.200.225

 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)? yes

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.

NP	Networks and Protocols (NP)	Prof. Dr. A. Grebe
CCNA SRWE	Switching, Routing, and Wireless Essentials (SRWE)	

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? Request time out

    How long was it interrupted?

c. 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?

d. 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.
    (Repeat tracert, if the path has not been changed yet.)

Checkout

When you successfully finished this Lab, record your solution.

1. Write your answers in red color into this PDF-File and save it as **SRWE-Lab2-Result.pdf**.

2. Save your final Packet Tracer file **SRWE-Lab2-PT.pkt**

3. Record the running configuration of switch S1, router R1, and router R2 (**show run**) in one text file **SRWE-Lab2-S1-R1-R2.txt**

4. Upload these 3 files as requested in 1.-3. in Ilias.

    Do NOT upload a ZIP-file or any other format.