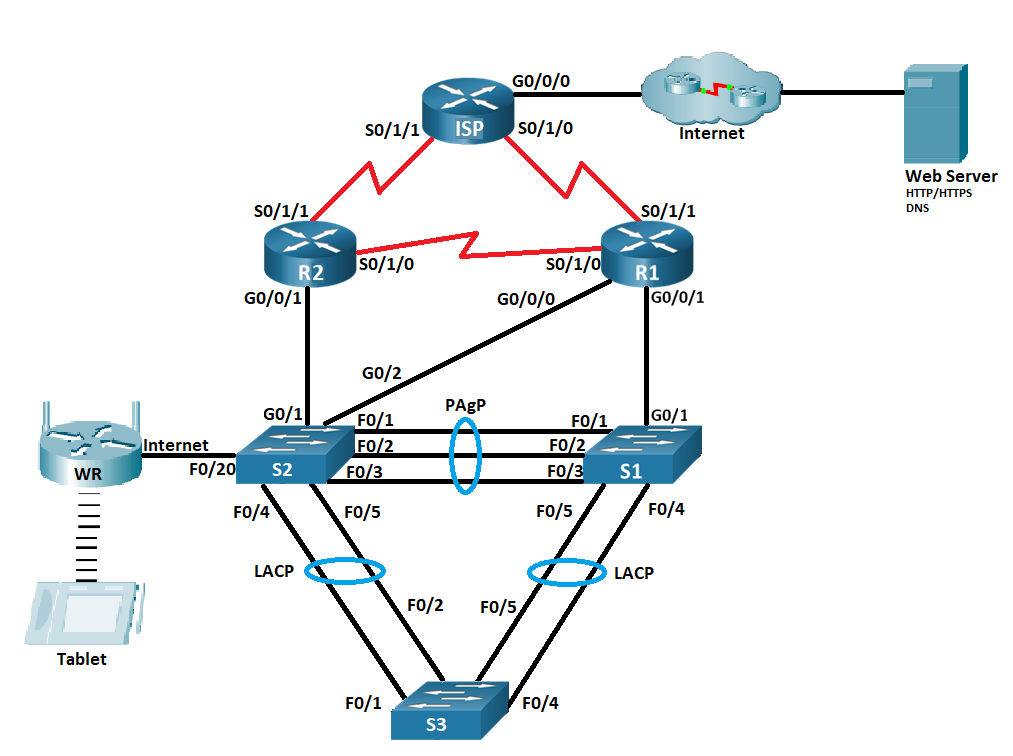
NTWK-2010 Final Project

# Topology



# Overview

For this project you are required to build a redundant network with EtherChannel, HSRP, Floating Static Routes, DHCP and Secure Wireless. You will then demonstrate that your end devices (Tablet and Laptop) can still access the Web Server and renew a DHCP lease even if either of the **ACTIVE** Router to Switch or ISP to Router links go down.

# Required Resources

* Laptop installed with Windows 10 or Mac OSX and connection to the Internet
* Packet Tracer version 8.0 or later

**Note:** Remember to frequently save your progress in packet tracer as it’s been known to crash.

# Objectives

Part 1: Label, Cable and Configure Basic Device Settings

Part 2: Create VLANs and Assign Switch Ports

Part 3: Configure 802.1Q Trunks and EtherChannel

Part 4: Configure Spanning-Tree Protocol

Part 5: Configure HSRP

Part 6: Configure Static Routes

Part 7: Configure DHCPv4, Stateful DHCPv6 and IP Helper Address

Part 8: Configure Network Security

Part 9: Implement Wireless Network

Part 10: Verify and test connectivity

# Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | Logical Network | Logical Host | Comment |
| Web Server | F0 | ---------------------------------- | 198.163.144.90 | Last Host |
| ISP | S0/1/0 | 203.0.113.64/30 |  | Last Host |
| S0/1/1 | 203.0.113.68/30 |  | Last Host |
| R1 | S0/1/1 | 203.0.113.64/30 |  | First Host |
| S0/1/0 | 172.31.0.0/30 |  | First Host |
| G0/0/0 | 2001:db8:acad:a::/64 | 2001:db8:acad:a::1 | GUA |
| fe80::/8 | fe80::1 | Link-Local |
| G0/0/1.10 | 10.1.1.0/25 |  | First Host |
| G0/0/1.11 | 10.1.1.128/25 |  | First Host |
| G0/0/1.12 | 10.1.2.0/24 |  | First Host |
| G0/0/1.13 | 10.1.3.0/24 |  | First Host |
| G0/0/1.15 | 10.1.5.0/27 |  | First Host |
| G0/0/1.1000 | N/A | N/A | Native |
| R2 | S0/1/1 | 203.0.113.68/30 |  | First Host |
| S0/1/0 | 172.31.0.0/30 |  | Last Host |
| G0/0/1.10 | 10.1.1.0/25 |  | Second Host |
| G0/0/1.11 | 10.1.1.128/25 |  | Second Host |
| G0/0/1.12 | 10.1.2.0/24 |  | Second Host |
| G0/0/1.13 | 10.1.3.0/24 |  | Second Host |
| G0/0/1.15 | 10.1.5.0/27 |  | Second Host |
| G0/0/1.1000 | N/A | N/A | Native |
| WR | Internet | 10.1.3.0/24 | DHCP | DHCP |
| Wireless | 192.168.100.0/24 |  | First Host |
| S1 | VLAN 15 | 10.1.5.0/27 |  | Second Last Host - SVI |
| S2 | VLAN 15 | 10.1.5.0/27 |  | Third Last Host - SVI |
| S3 | VLAN 15 | 10.1.5.0/27 |  | Fourth Last Host - SVI |

# VLAN Table

|  |  |  |
| --- | --- | --- |
| VLAN | Name | Interface Assigned |
| 10 | Sales | S1: F0/6-9  S2: F0/6-9  S3: F0/6-9 |
| 11 | Finance | S1: F0/11-14  S2: F0/11-14  S3: F0/11-14 |
| 12 | Server | S1: F0/16-17  S2: F0/16-17  S3: F0/16-17 |
| 13 | Wireless | S1: F0/20-21  S2: F0/20-21  S3: F0/20-21 |
| 15 | Management | S1: F0/22-23  S2: F0/22-23  S3: F0/22-23 |
| 50 | Research | S1: F0/24  S2: G0/2, F0/24  S3: F0/24 |
| 999 | ParkingLot | Unused Ports |
| 1000 | Native | N/A |

# Instructions

## Label, Cable and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the routers and switches.

### Setup the network as shown in the topology

1. Drag and rename network devices into blank space in logical topology

Note: For routers use model 4321. For switches use model 2960. For WR use model WRT300N.

1. From the physical tab on R1 and R2, drag a NIM-2T module in an empty expansion slot (see [Figure.1](#_Appendix))
2. Attach cables to the devices as shown in the topology diagram.

Note: Connect Serial DCE cables to ISP router interfaces (see [Figure.2)](#_Appendix).

### Configure basic settings for each switch and router

* + - 1. Assign a device name to the device.
      2. Disable DNS lookup.
      3. Assign **class1234!** as the privileged EXEC encrypted password.
      4. Configure username **admin** and password **cisco1234!.**
      5. Use local login authentication for console access.
      6. Use local login authentication for vty access.
      7. Enable **only** SSH access. Use SSH version 2.
      8. Encrypt the plaintext passwords.
      9. Create a banner that warns anyone accessing the device that unauthorized access is prohibited and to contact your academic email for access.
      10. Copy the running configuration to the startup configuration.

### Configure R1 and R2 Interfaces

1. Configure R1 and R2 interfaces using the IP address information in the Addressing Table above.

**Note:** VLAN 1000 is the native VLAN.

1. Configure IPv6 unicast routing on R1
2. Document all active interfaces with descriptions.

Close configuration window

## Create VLANs and Assign Switch Ports

### Create VLANs on all switches.

Open configuration window

* + - 1. Create and name the required VLANs on each switch from the table above.
      2. Configure SVI’s on each switch using the IP address information in the Addressing Table.

### Assign VLANs to the correct switch interfaces.

* + - 1. Assign switchports to the appropriate VLAN (specified in the VLAN table above) and configure them for static access mode.
      2. Document all active interfaces with descriptions.
      3. Verify that the VLANs are assigned to the correct interfaces.

Close configuration wi

## Configure an 802.1Q Trunks and EtherChannel

### Manually configure trunk interface on switchport uplinks

* + - 1. Configure switchport mode on each switch to switch and switch to router uplink interface (except S2 G0/2) to force trunking. Make sure to do this on all switches.
      2. Set the native VLAN to 1000 on all trunks.
      3. As another part of trunk configuration, specify that only VLANs 10, 11, 12, 13, 15, 50 and 1000 are allowed to cross the trunk.
      4. Disable DTP (Dynamic Trunking Protocol) on all trunk interfaces.
      5. Issue the appropriate show command to verify trunking ports, the native VLAN and allowed VLANs across the trunk.

### Configure EtherChannel

* + - 1. Create a PAgP-EtherChannel unconditionally using group number 1 between S1 and S2. Reference the topology to know which switchport interfaces to bundle.
      2. Create a LACP EtherChannel unconditionally using group number 2 between S1 and S3. Reference the topology to know which switchport interfaces to bundle.
      3. Create a LACP EtherChannel unconditionally using group number 3 between S2 and S3. Reference the topology to know which switchport interfaces to bundle.
      4. Use the appropriate show command to verify the EtherChannel configuration.

**Note:** Reloading the switches may be necessary to bring up port-channels after configuration is complete.

## Configure Spanning-Tree Protocol

### Configure STP on S1, S2 and S3

1. Set spanning-tree mode to rapid-pvst.
2. Set S1 as the root bridge for VLAN 12.
3. Set S2 as the root bridge for VLAN 13.
4. Set S3 as the root bridge for remaining VLANs.
5. Prevent other switches from being connected to all access mode ports (except VLAN 999).
6. All access ports should also move directly to forwarding state on link up (except VLAN 999).

Close configuration window

## Configure HSRP

### Implement HSRP on R1 and R2

1. Configure HSRP groups for VLAN 10, 11, 12, 13 and 15 with R1 as active and R2 as standby.

* Active router priority should be 105. Standby router priority is default value.
* If link between R1 and S1 is shutdown, R2 should takeover active state.
* If link between R1 to S1 comes back up, R1 should takeover active state.
* Configure Virtual IP (VIP) as last usable host for VLAN 10, 11, 12, 13 and 15

### Configure default gateway IP on S1, S2 and S3

1. Configure an IP default gateway on S1, S2 and S3. Be sure to use the virtual gateway IP configured on VLAN 15 (Management).

## Configure Static Routes

### Configure R1 routes

1. Configure an IPv4 static default route via next-hop IP address of ISP router.
2. Configure an IPv4 floating static default route via next-hop IP address of S0/1/0 on R2.
3. Configure an IPv4 static route summarizing VLAN 10, 11, 12, 13 and 15 networks via next-hop IP address of S0/1/0 on R2.

### Configure R2 routes

1. Configure an IPv4 static default route via next-hop IP address of ISP router.
2. Configure an IPv4 floating static default route via next-hop IP address of S0/1/0 interface on R1.
3. Configure an IPv4 static route summarizing VLAN 10, 11, 12, 13 and 15 networks via next-hop IP address of S0/1/0 on R1.

## Configure DHCPv4, Stateful DHCPv6 and IP Helper Address

### Configure R1 with DHCP pools for VLAN 10 and 11

* + - 1. Exclude the first and last 10 useable addresses from each address pool.
      2. Create DHCP pool using the VLAN name.
      3. Specify the network address and subnet mask that this DHCP server is supporting.
      4. Configure the domain name as rrc.ca
      5. Configure the appropriate default gateway.
      6. Set name server (DNS) to Web Server IP address.

### Configure R2 with DHCP pools for VLAN 13 and 15

* + - 1. Exclude the first and last 5 useable addresses from each address pool.
      2. Create DHCP pool using the VLAN name.
      3. Specify the network address and subnet mask that this DHCP server is supporting.
      4. Configure the domain name as rrc.ca
      5. Configure the appropriate default gateway.
      6. Set name server (DNS) to Web Server IP address.

### Configure R1 sub-interfaces with IP helper address

1. Apply the ip helper-address command under sub-interfaces on R1 specifying R2’s S0/1/0 IP address. Do this only for networks where R2 hosts the DHCP pool (VLAN 13 and 15)

### Configure R2 sub-interfaces with IP helper address

1. Apply the ip helper-address command under sub-interfaces on R2 specifying R1’s S0/1/0 IP address. Do this only for networks where R1 hosts the DHCP pool (VLAN 10 and 11)

### Configure a stateful DHCPv6 server on R1

* + - 1. Create a DHCPv6 pool on R1 with the name “**R1-STATEFUL**”.
      2. GUA prefix allocation requires 48 host bits.
      3. Set the DNS server to 2001:db8:acad:a::254
      4. Set the domain name to rrc.ca
      5. Enable IPv6 dhcp server on G0/0/0 interface on R1

## Configure Network Security

### Unused switchport configuration on S1, S2 and S3

1. Set unused ports to access mode on VLAN 999 and shutdown

### Configure port-security on S1, S2 and S3

1. Enable port-security on access ports for VLAN 10, 11 and 15.
2. Allow only two mac addresses to be learned on access ports for VLAN 10, 11, and 15
3. Configure VLAN 10, 11 and 15 access ports to add MAC addresses learned on the port automatically to the running configuration.

### Configure security best practices on R1 and R2

1. Set a minimum password length of 8 characters
2. Block VTY access for 5 minutes if 3 or more failed login attempts have been made within 60 seconds.

## Implement Wireless Network

### Initial configuration of WR

1. Login to the GUI of WR
2. Update the Router password to cisco1234!

**Note:** Be sure to Save Settings at the bottom of the page every time a configuration change is made.

1. Create a wireless network with an SSID of “Guest” and disable the SSID Broadcast
2. Apply the following wireless security to the Guest network:
   * 1. Security Mode: WPA2 Personal
     2. Encryption: AES
     3. Passphrase: guest1234!

### Connect Tablet to Guest wireless network

1. Under the Wireless0 interface of the tablet, update the SSID and authentication method to connect to the Guest wireless network.

## Verify and test connectivity

1. Connect a laptop to access ports on VLAN 10, 11, 13 and 15 on each switch and verify host gets IPv4 settings via DHCP. Once a lease is obtained, try the following:
   1. SSH to R1, R2, S1, S2 and S3.
   2. Ping the virtual gateway IP for each VLAN.
   3. Access the HTTP and HTTPS service on the Web Server via IPv4 address and domain-name (www.rrc.ca).
2. Connect a laptop to an access port on VLAN 50 and verify host gets IPv6 settings via DHCPv6. Once IPv6 GUA is obtained, try to ping the following:
   1. R1 G0/0/0 interface
3. Verify the Tablet is able to access
   * Access the HTTP and HTTPS service on the Web Server via IPv4 address and domain-name (www.rrc.ca).
4. Disconnect the link between R1 and S1 then repeat steps in Part 10 a.
5. Disconnect the link between R2 and ISP then repeat steps in Part 10 a 3.
6. Reconnect the link between R1 and S1
7. Reconnect the link between R2 and ISP
8. Disconnect the link between R1 and ISP then repeat the steps in Part 10 a 3

Note: Assessment Items will become visible once score of 90% or higher is achieved.

1. If all tests succeed, upload Final Project.pka and this document to Final Project dropbox in LEARN.

# Appendix

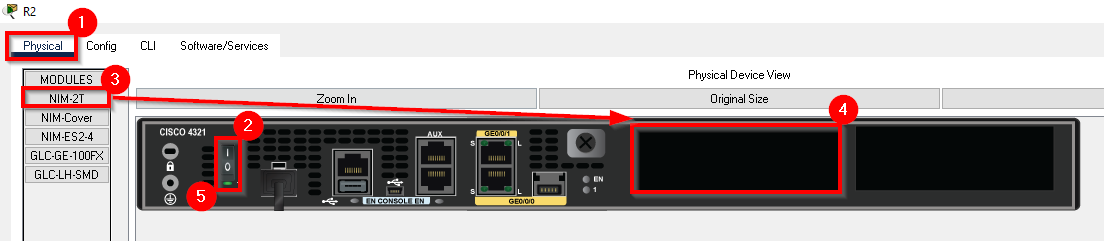


Figure 1

S2 

Figure 2

Last revised July 2021