

Packet Tracer - Basic Device Configuration

Addressing Table

Device	Interface	IP Address	Default Gateway
[[R1Name]]	G0/0	[[R1G0Add]]/24	N/A
		[[R1G0Addv6]]/64	
		[[R1G0Addv6LL]]	
	G0/1	[[R1G1Add]]/24	N/A
		[[R1G1Addv6]]/64	
		[[R1G1Addv6LL]]	
[[S1Name]]	VLAN 1	[[S1Add]]/24	[[R1G0Add]]
[[S2Name]]	VLAN 1	[[S2Add]]/24	[[R1G1Add]]
[[PC1Name]]	NIC	[[PC1Add]]/24	[[R1G0Add]]
		[[PC1Addv6]]/64	[[R1G0Addv6LL]]
[[PC2Name]]	NIC	[[PC2Add]]/24	[[R1G0Add]]
		[[PC2Addv6]]/64	[[R1G0Addv6LL]]
[[PC3Name]]	NIC	[[PC3Add]]/24	[[R1G1Add]]
		[[PC3Addv6]]/64	[[R1G1Addv6LL]]
[[PC4Name]]	NIC	[[PC4Add]]/24	[[R1G1Add]]
		[[PC4Addv6]]/64	[[R1G1Addv6LL]]

Objectives

- Complete the network documentation.
- Perform basic device configurations on a router and a switch.
- Verify connectivity and troubleshoot any issues.

Scenario

Your network manager is impressed with your performance in your job as a LAN technician. She would like you to demonstrate your ability to configure a router that connects two LANs. Your tasks include configuring basic settings on a router and a switch using the Cisco IOS. You will also configure IPv6 addresses on network devices and hosts. You will then verify the configurations by testing end-to-end connectivity. Your goal is to establish connectivity between all devices.

Note: The VLAN1 interface on [[S1Name]] will not be reachable over IPv6.

In this activity you will configure the [[R1Name]] router, [[S2Name]] switch, and the **PC** hosts.

Note: Packet Tracer will not score some configured values, however these values are required to accomplish full connectivity in the network.

Requirements

- Provide the missing information in the Addressing Table.
Note: Some of the information is provided in the Packet Tracer instructions for your topology.
 - Name the router **[[R1Name]]** and the second switch **[[S2Name]]**. You will not be able to access the **[[S1Name]]** switch.
 - Use **cisco** as the user EXEC password for all lines.
 - Use **class** as the encrypted privileged EXEC password.
 - Encrypt all plaintext passwords.
 - Configure an appropriate banner.
 - Configure IPv4 and IPv6 addressing for the **[[R1Name]]** switch according to the Addressing Table.
 - Configure IPv4 and IPv6 addressing for the **[[S2Name]]** switch according to the Addressing Table.
 - The hosts are partially configured. Complete the IPv4 addressing, and fully configure the IPv6 addresses according to the Addressing Table.
 - Document interfaces with descriptions, including the **[[S2Name]]** VLAN 1 interface.
 - Save your configurations.
 - Verify connectivity between all devices. All devices should be able to ping all other devices with IPv4 and IPv6.
 - Troubleshoot and document any issues.
 - Implement the solutions necessary to enable and verify full end-to-end connectivity.
-

Scenario 1 (ID: 000)

Router College

```
service password-encryption
hostname College
enable secret class
ipv6 unicast-routing
interface GigabitEthernet0/0
  description Connection to Class-A
  ip address 128.107.20.1 255.255.255.0
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:A::1/64
  no shutdown
interface GigabitEthernet0/1
  description Connection to Class-B
  ip address 128.107.30.1 255.255.255.0
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:B::1/64
  no shutdown
banner motd "Warning: Unauthorized Access Prohibited."
line con 0
  password cisco
  login
line vty 0 4
  password cisco
  login
do copy run start
```

Switch Class-B

```
service password-encryption
hostname Class-B
enable secret class
interface Vlan1
  description Connection to College g0/1
  ip address 128.107.30.15 255.255.255.0
  no shutdown
banner motd "Warning: Unauthorized Access Prohibited."
line con 0
  password cisco
  login
line vty 0 4
  password cisco
  login
do copy run start
```

Scenario 2 (ID: 111)

Router Floor14

```
service password-encryption
hostname Floor14
enable secret class
ipv6 unicast-routing
interface GigabitEthernet0/0
  description Connection to Room-145
  ip address 172.14.5.1 255.255.255.0
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:CAFE:1::1/64
  no shutdown
interface GigabitEthernet0/1
  description Connection to Room-146
  ip address 172.14.10.1 255.255.255.0
  ipv6 address FE80::2 link-local
  ipv6 address 2001:DB8:CAFE:2::1/64
  no shutdown
banner motd "Warning: Unauthorized Access Prohibited."
line con 0
  password cisco
  login
line vty 0 4
  password cisco
  login
do copy run start
```

Switch Room-146

```
service password-encryption
hostname Room-146
enable secret class
interface Vlan1
  description Connection to Floor14 g0/1
  ip address 172.14.10.35 255.255.255.0
  no shutdown
banner motd "Warning: Unauthorized Access Prohibited."
line con 0
  password cisco
  login
line vty 0 4
  password cisco
  login
do copy run start
```

Scenario 3 (ID: 222)

Router RTA

```
service password-encryption
hostname RTA
enable secret class
ipv6 unicast-routing
interface GigabitEthernet0/0
  description Connection to ASw-1
  ip address 10.10.10.1 255.255.255.0
  ipv6 address FE80::2 link-local
  ipv6 address 2001:DB8:ACAD:100::1/64
  no shutdown
interface GigabitEthernet0/1
  description Connection to ASw-2
  ip address 10.10.11.1 255.255.255.0
  ipv6 address FE80::3 link-local
  ipv6 address 2001:DB8:ACAD:200::1/64
  no shutdown
banner motd "Warning: Unauthorized Access Prohibited."
line con 0
  password cisco
  login
line vty 0 4
  password cisco
  login
do copy run start
```

Switch ASw-2

```
service password-encryption
hostname ASw-2
enable secret class
interface Vlan1
  description Connection to RTA g0/1
  ip address 10.10.11.100 255.255.255.0
  no shutdown
banner motd "Warning: Unauthorized Access Prohibited."
line con 0
  password cisco
  login
line vty 0 4
  password cisco
  login
do copy run start
```