**Advanced Diploma of Information Technology**

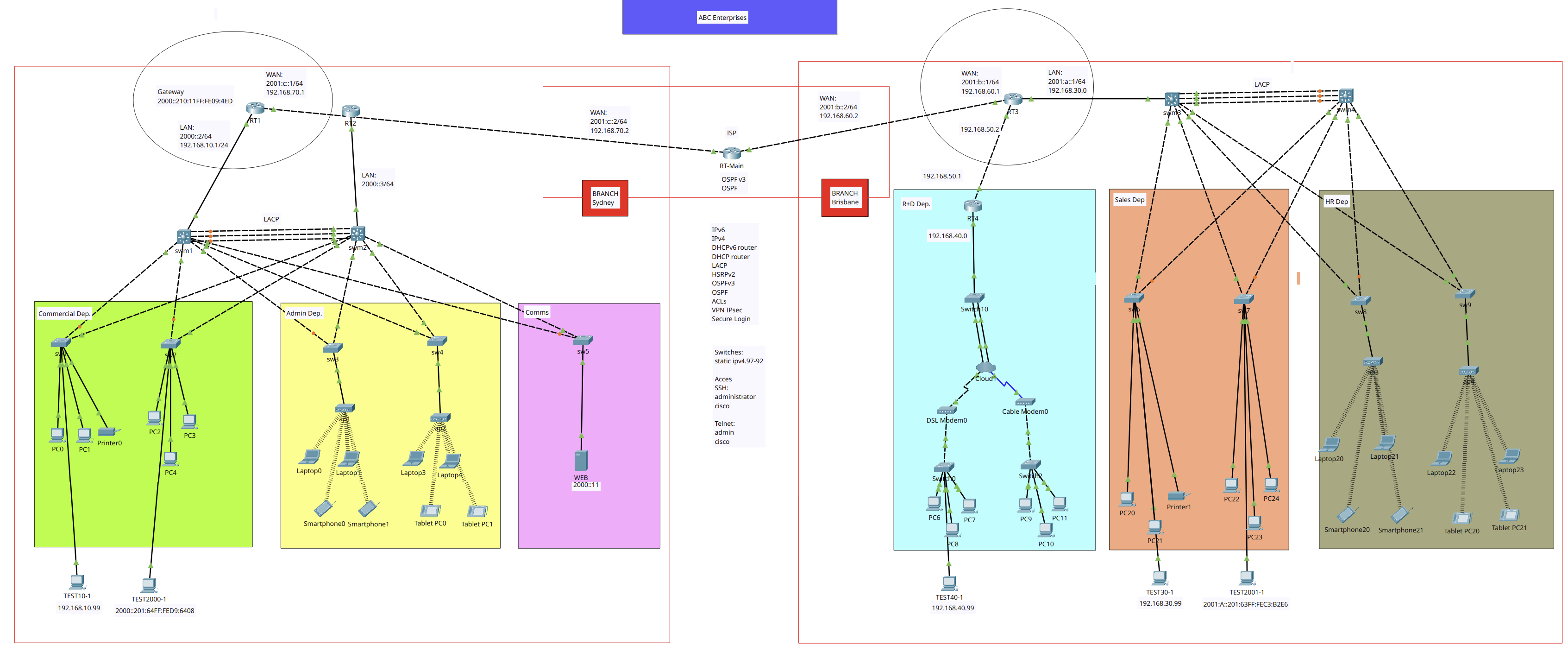
**ICTNWK541 Assessment**

**Assessment Task 2: Project Portfolio**

**Manuel Sergio Perez Espitia**

**March 20th 2025, Melbourne, Victoria, Australia**

**ABC Enterprises WAN Expansion**



ABC Enterprises is a growing company with headquarters in Melbourne and two branch offices in Sydney and Brisbane. The company currently operates with an outdated network infrastructure that lacks secure, reliable WAN connectivity between sites. The IT department has been tasked with designing, implementing, and securing a new WAN infrastructure that ensures:

* Secure VPN connectivity between all sites.
* Optimised bandwidth usage with reliable routing protocols.
* Proper IPv6 deployment for future scalability.
* Enhanced security mechanisms including firewall rules and access control lists (ACLs).
* Troubleshooting and monitoring tools to detect and rectify network issues efficiently.

As part of the project, you will act as a network engineer responsible for implementing the required WAN connectivity for ABC Enterprises.

# Simulation Software & Tools:

Software installed to develop this protect.

* Cisco Packet Tracer 8.2.2
* Ubuntu 24.04 LTS
* Wireshark 4.2.2

# Network Design Review & Planning

## Network Details

### Topology and type

* Sydney Branch:
  + Type: WAN
  + Topology: Dual-Star high availability
  + Architecture: 3-Tier
* Brisbane Branch:
  + Type: LAN
  + Topology: Star

### Network Nodes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device** | **Name** | **Network** | **Device** | **Name** | **Network** |
| **Router 1** | RT1 | Sydney | **Router 2** | RT2 | Sydney |
| **Switch 1** | sw1 | Sydney | **Switch 2** | sw2 | Sydney |
| **Switch 3** | sw3 | Sydney | **Switch 4** | sw4 | Sydney |
| **Switch 5** | sw5 | Sydney | **Switch ML1** | sw11 | Sydney |
| **Switch ML2** | sw12 | Sydney | **Router 3** | RT3 | Brisbane |
| **Router 4** | RT4 | Brisbane | **Switch 6** | sw6 | Brisbane |
| **Switch 7** | sw7 | Brisbane | **Switch 8** | sw8 | Brisbane |
| **Switch 9** | sw9 | Brisbane | **Switch 10** | sw10 | Brisbane |
| **Switch ML3** | sw13 | Brisbane | **Switch ML4** | sw14 | Brisbane |
| **Router Main** | **RT-M** | **ISP** | **-** | **-** | **-** |

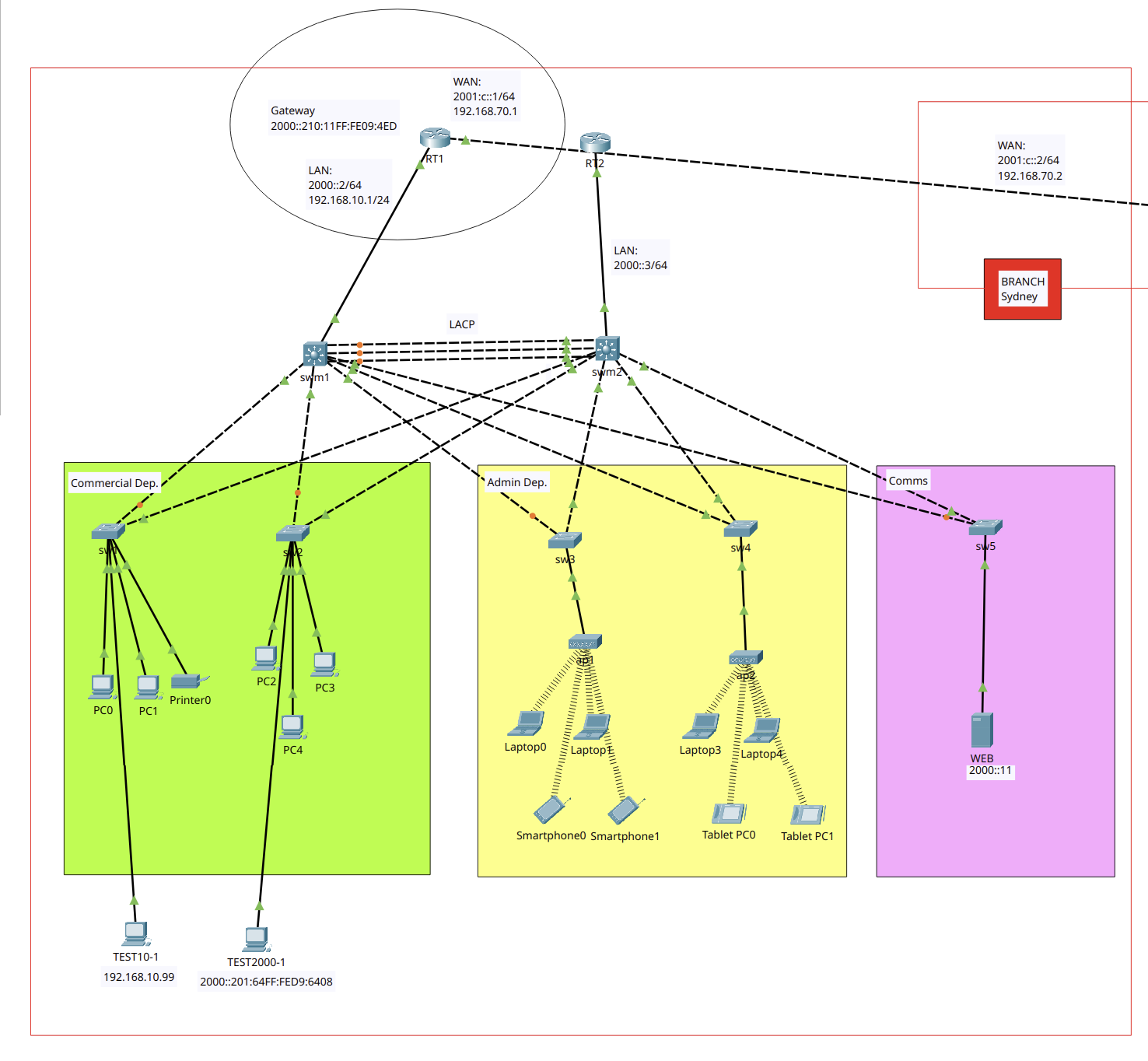
### Network Details – Sydney Branch

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Details | Protocols IPv6 | Protocols IPv4 | Access |
| RT-M | WAN: 2001:c::2/64 192.168.70.2 | OSPFv3 | OSPF | Password Encryption  (RSA)   Local: admin  SSH: administrator cisco  Telnet:  admin Cisco |
| RT1 | WAN: 2001:c::1/64 192.168.70.1  LAN: 2000::2/64 192.168.10.1/24  Gateway 2000::210:11FF:FE09:4ED 192.168.10.99  DNS: 2000::10 192.168.10.10 | DHCPv6 router HSRPv2 OSPFv3 | DHCP router VPN Ipsec ACL |
| RT2 | LAN: 2000::3/64  Gateway: FE80::290:21FF:FE69:EC83  DNS: 2000::10 | DHCPv6 router HSRPv2 | DHCP router |
| swm1 | VLAN1: 192.168.10.97 | LAC |  |
| swm2 | VLAN1: 192.168.10.98 | LAC |  |
| sw1 | VLAN1: 192.168.10.96 |  |  |
| sw2 | VLAN1: 192.168.10.95 |  |  |
| sw3 | VLAN1: 192.168.10.94 |  |  |
| sw4 | VLAN1: 192.168.10.93 |  |  |
| sw5 | VLAN1: 192.168.10.92 |  |  |

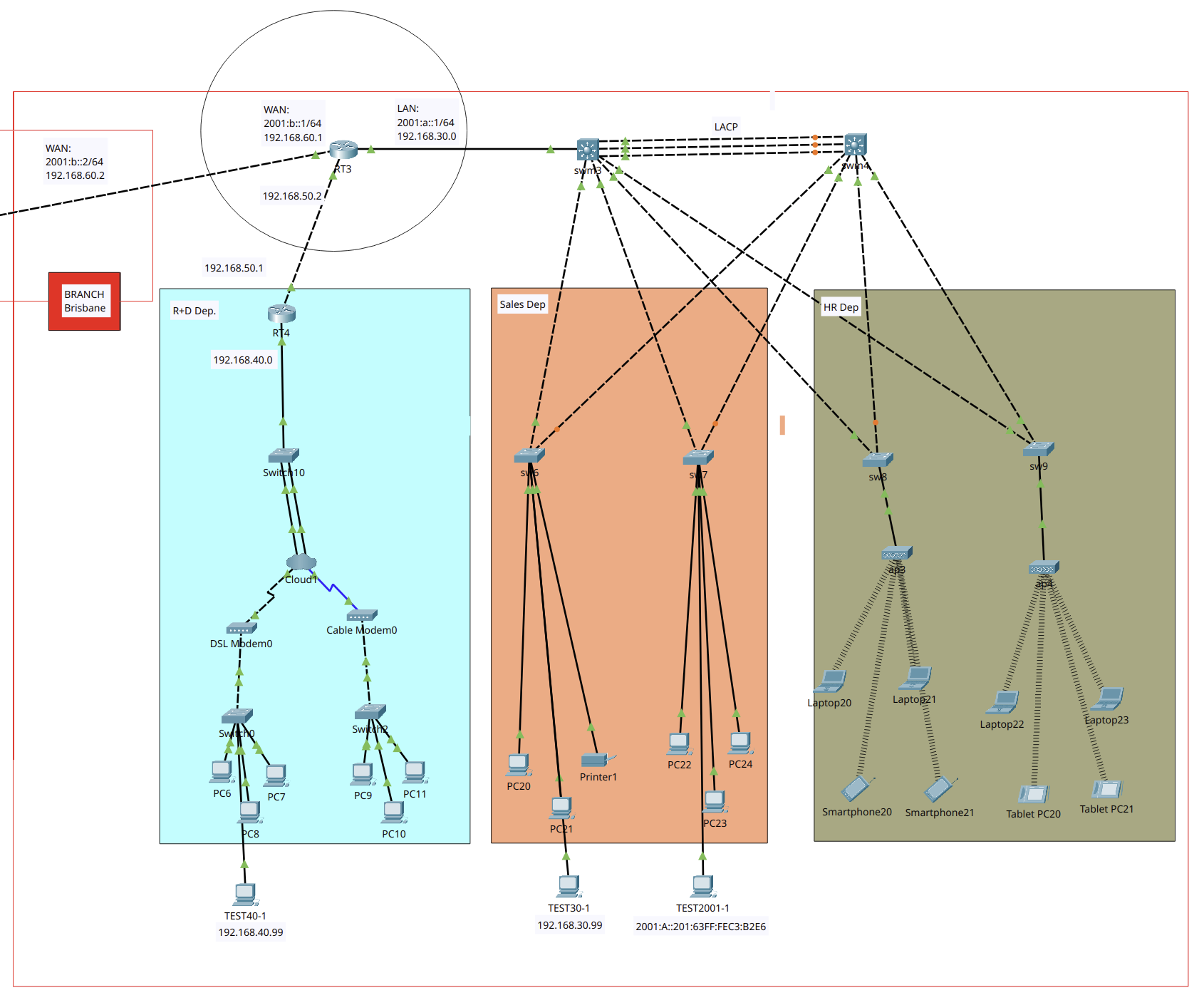
### Network Details – Brisbane Branch

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Details | Protocols IPv6 | Protocols IPv4 | Access |
| RT-M | WAN: 2001:b::2/64 192.168.60.2 | OSPFv3 | OSPF | Password Encryption  (RSA)   Local: admin  SSH: administrator cisco  Telnet:  admin Cisco |
| RT3 | WAN: 2001:b::1/64 192.168.60.1  LAN: 2001:a::1/64 192.168.30.0  Gateway FE80::20C:CFFF:FE8B:7037  DNS: 2001:a::10 192.168.30.10 | DHCPv6 router HSRPv2 OSPFv3 | DHCP router VPN Ipsec ACL |
| RT4 | LAN: 192.168.40.0  Gateway: 192.168.40.1  DNS: 192.168.40.10 |  | DHCP router |
| swm3 | VLAN1: 192.168.30.97 | LAC |  |
| swm4 | VLAN1: 192.168.30.98 | LAC |  |
| sw6 | VLAN1: 192.168.30.96 |  |  |
| sw7 | VLAN1: 192.168.30.95 |  |  |
| sw8 | VLAN1: 192.168.30.94 |  |  |
| sw9 | VLAN1: 192.168.30.93 |  |  |
| sw10 | VLAN1: 192.168.40.92 |  |  |

### Sydney Branch Network



### Brisbane Branch Network



# WAN Configuration

## Installation Plan

1. Implement Network Topology
2. Implement Secure Access by SSH & Telnet
3. Implement Additional Protocols: DHCPv6, IPV6
4. Implement Additional Protocols: LACP
5. Implement Additional Protocols: HSRPv2 IPv6
6. Implement Additional Protocols: WEB Server
7. Implement Additional Protocols: OSPFv3
8. Implement Additional Protocols: DualStack, DHCP
9. Implement Additional Protocols: OSPF
10. Implement WAN protocols: Extended Access Control List (ACL)
11. Implement WAN Protocols: VPN Site-To-Site over IPv4
12. Implement WAN Protocols: Encapsulation PPP over IPv4

## Legal & security: Policies and Procedures

1. Service Password Encryption
2. Mandatory Login Password
3. VPN Site-to-Site
4. Access Control Lists (ACLs)
5. Secure Remote Access to infrastructure

## Troubleshooting & Testing

1. Testing LAN Connectivity (IPv4/IPv6)
2. Testing WAN Connectivity (IPv4/IPv6)
3. Testing Secure Access SSH & Telnet - Local
4. Testing DHCP/DHCPv6 (IPv4/IPv6)
5. Testing LACP (IPv6)
6. Testing HSRPv2 (IPv6)
7. Testing OSPF/OSPFv3 (IPv4/IPv6)
8. Testing ACL (IPv4)
9. Testing VPN Site-To-Site (IPv4)
10. Testing Encapsulation PPP (IPv4)
11. Testing Firewall & Single-port

## Summary Technologies & Protocols

## Bibliography

# WAN Configuration

## Installation Plan

## Implement Network Topology

Rename all devices:

|  |  |  |  |
| --- | --- | --- | --- |
| **Device Type** | **Quantity** | **Device Type** | **Quantity** |
| Router | 5 | **Switch** | 14 |
| PC | 20 | **Laptop** | 8 |
| Smartphone | 4 | **Tablet** | 4 |
| Server | 1 | **Printer** | 2 |
| W Access Point | 4 | **Modem** | 2 |

## 3. Additional Protocols: DHCPv6, IPV6

### Router 1 (RT1)

Firstly, IPv6 will be enable and then DHCPv6 will be set up

enable

configure terminal

hostname RT1

ipv6 unicast-routing

interface gigabitEthernet 0/0

ipv6 address 2000::2/64

no shutdown

ipv6 dhcp pool STATEFUL\_POOL

domain-name milestones.com

dns-server 2000::10

prefix-delegation pool STATEFUL\_POOL

exit

interface gigabitEthernet 0/0

ipv6 dhcp server STATEFUL\_POOL

ipv6 nd managed-config-flag

exit

Do wr

exit

exit

### Router 3 (RT3)

enable

configure terminal

hostname RT3

ipv6 unicast-routing

interface gigabitEthernet 0/2

ipv6 address 2001:a::1/64

no shutdown

ipv6 dhcp pool STATEFUL\_POOL

domain-name milestones.com

dns-server 2001:a::10

prefix-delegation pool STATEFUL\_POOL

exit

interface gigabitEthernet 0/2

ipv6 dhcp server STATEFUL\_POOL

ipv6 nd managed-config-flag

exit

Do wr

exit

exit

## 4. Implement Additional Protocols: LACP

Implementation of Link Aggregation Control Protocol (LACP) on links:

* swm1 gigabitEthernet 1/0/22 <—> swm2 gigabitEthernet 1/0/22
* swm1 gigabitEthernet 1/0/23 <—> swm2 gigabitEthernet 1/0/23
* swm1 gigabitEthernet 1/0/24 <—> swm2 gigabitEthernet 1/0/24
* swm3 gigabitEthernet 1/0/22 <—> swm4 gigabitEthernet 1/0/22
* swm3 gigabitEthernet 1/0/23 <—> swm4 gigabitEthernet 1/0/23
* swm3 gigabitEthernet 1/0/24 <—> swm4 gigabitEthernet 1/0/24

The LACP link will be the **channel-group** number **1** on all switches.

### Switch Main 1 (swm1)

enable

configure terminal

interface range gigabitEthernet 1/0/22, gigabitEthernet 1/0/23, gigabitEthernet 1/0/24

channel-group 1 mode active

exit

interface Port-channel 1

switchport mode trunk

exit

do wr

exit

exit

enable

configure terminal

interface gigabitEthernet 1/0/1

switchport

no shutdown

Exit

Do wr

exit

### Switch Main 2 (swm2)

enable

configure terminal

interface range gigabitEthernet 1/0/22, gigabitEthernet 1/0/23, gigabitEthernet 1/0/24

channel-group 1 mode passive

exit

interface Port-channel 1

switchport mode trunk

exit

do wr

exit

exit

enable

configure terminal

interface gigabitEthernet 1/0/1

switchport

no shutdown

Exit

Do wr

exit

### Switch Main 3 (swm3)

enable

configure terminal

interface range gigabitEthernet 1/0/22, gigabitEthernet 1/0/23, gigabitEthernet 1/0/24

channel-group 1 mode active

exit

interface Port-channel 1

switchport mode trunk

exit

do wr

exit

exit

enable

configure terminal

interface gigabitEthernet 1/0/1

switchport

no shutdown

Exit

Do wr

exit

### Switch Main 4 (swm4)

enable

configure terminal

interface range gigabitEthernet 1/0/22, gigabitEthernet 1/0/23, gigabitEthernet 1/0/24

channel-group 1 mode passive

exit

interface Port-channel 1

switchport mode trunk

exit

do wr

exit

exit

enable

configure terminal

interface gigabitEthernet 1/0/1

switchport

no shutdown

Exit

Do wr

exit

## 5. Implement Additional Protocols: HSRPv2 IPv6

Links:

* HSRP IPv6 Address: 2000::1/64
* RT1 gigabitEthernet 0/0 <—> 2000::2 (primary router)
* RT2 gigabitEthernet 0/0 <—> 2000::3 (secondary router)

Checking

* show running-config | include standby
* show standby

### Router 1 (RT1)

enable

configure terminal

interface gigabitEthernet 0/0

ipv6 address 2000::2/64

standby version 2

standby 1 ipv6 autoconfig

standby 1 priority 120

no shutdown

Exit

Do wr

exit

exit

### Router 2 (RT2)

Firstly, It will be setting up RT2 same as RT1 then RT2 will be marked as a secondary router.

enable

configure terminal

hostname RT2

ipv6 unicast-routing

interface gigabitEthernet 0/0

ipv6 address 2000::3/64

no shutdown

ipv6 dhcp pool STATEFUL\_POOL

domain-name milestones.com

dns-server 2000::10

prefix-delegation pool STATEFUL\_POOL

exit

interface gigabitEthernet 0/0

ipv6 dhcp server STATEFUL\_POOL

ipv6 nd managed-config-flag

exit

Do wr

exit

exit

enable

configure terminal

interface gigabitEthernet 0/0

ipv6 address 2000::3/64

standby version 2

standby 1 ipv6 autoconfig

no shutdown

Exit

Do wr

exit

exit

## 6. Additional Protocols: WEB Server

Firstly, enable HTTP and HTTPs services and disable all other services, then edit index.html

<html>

<center><font size='+2' color='blue'>ABC ENTERPRISES Sydney</font></center>

<hr>Welcome to ABC Enterprises WEB server. This is a project for an assessment task 2 - May 2025.

<p>Quick Links:

<br><a href='helloworld.html'>A small page</a>

<br><a href='copyrights.html'>Copyrights</a>

<br><a href='image.html'>Image page</a>

<br><a href='cscoptlogo177x111.jpg'>Image</a>

</html>

## 7. Additional Protocols: OSPFv3

Links:

* RT1 Network gigabitEthernet 0/0
* RT1 gigabitEthernet 0/1 <—> RT-M gigabitEthernet 0/0
* RT3 Network gigabitEthernet 0/2
* RT-M gigabitEthernet 0/2 <—> RT-3 gigabitEthernet 0/1

Addressing:

* RT1 —> 2000::2/64
* RT1 <—> RT-M, 2001:c::1/64
* RT-M <—> RT1, 2001:c::2/64
* RT3 —> 2001:a::1/64
* RT-M <—> RT3, 2001:b::2/64
* RT3 <—> RT-M, 2001:b::1/64

Checking, reload:

* show ipv6 ospf neighbor
* clear ipv6 ospf process
* Show ipv6 ospf database

### Router 1 (RT1)

**!general config, IP link**

enable

configure terminal

interface gigabitEthernet 0/1

ipv6 address 2001:c::1/64

no shutdown

exit

**!enabling unicast and giving id**

ipv6 unicast-routing

ipv6 router OSPF 10

router-id 1.1.1.1

exit

**!enabling OSPF on network link**

interface gigabitEthernet 0/0

ipv6 OSPF 10 area 0

exit

**!enabling OSPF between RT1 and RT-M**

interface gigabitEthernet 0/1

ipv6 OSPF 10 area 0

exit

do wr

### Router Main (RT-Main)

**!general config, IP link**

enable

configure terminal

interface gig0/0

ipv6 address 2001:c::2/64

no shutdown

exit

interface gig0/2

ipv6 address 2001:b::2/64

no shutdown

exit

**!enabling unicast and giving router id**

ipv6 unicast-routing

ipv6 router OSPF 10

router-id 2.2.2.2

exit

**!enabling OSPF between RT-Main and RT1**

interface gig0/0

ipv6 OSPF 10 area 0

exit

**!enabling OSPF between RT-Main and RT3**

interface gig0/2

ipv6 OSPF 10 area 0

exit

do wr

### Router 3 (RT3)

**!general config, IP link**

enable

configure terminal

interface gigabitEthernet 0/1

ipv6 address 2001:b::1/64

no shutdown

exit

**!enabling unicast and giving router id**

ipv6 unicast-routing

ipv6 router OSPF 10

router-id 3.3.3.3

exit

**!enabling OSPF on network link**

interface gigabitEthernet 0/2

ipv6 OSPF 10 area 0

exit

**!enabling OSPF between RT3 and RT-Main**

interface gigabitEthernet 0/1

ipv6 OSPF 10 area 0

exit

do wr

exit

## 8. Implement Additional Protocols: DualStack, DHCP

### Router 1 (RT1)

**!setting up IPv4, dhcp**

enable

configure terminal

do wr

interface gigabitEthernet 0/0

ip address 192.168.10.1 255.255.255.0

no shutdown

exit

do wr

ip dhcp pool STATEFUL\_POOL

network 192.168.10.0 255.255.255.0

default-router 192.168.10.1

dns-server 192.168.10.10

exit

do wr

### Router 3 (RT3)

**!setting up ipv4, dhcp**

enable

configure terminal

do wr

interface gigabitEthernet 0/2

ip address 192.168.30.1 255.255.255.0

no shutdown

exit

do wr

ip dhcp pool STATEFUL\_POOL

network 192.168.30.0 255.255.255.0

default-router 192.168.30.1

dns-server 192.168.30.10

exit

do wr

### Router 4 (RT4)

Enabling IPv4 to ensure full compatibility with DSL protocol connection.

**!setting up IPv4, dhcp**

enable

configure terminal

hostname RT4

do wr

interface gigabitEthernet 0/0

ip address 192.168.40.1 255.255.255.0

no shutdown

exit

do wr

ip dhcp pool STATEFUL\_POOL

network 192.168.40.0 255.255.255.0

default-router 192.168.40.1

dns-server 192.168.40.10

exit

do wr

## 9. Additional Protocols: OSPF

Links:

* RT1 Network gigabitEthernet 0/0
* RT1 gigabitEthernet 0/1 <—> RT-M gigabitEthernet 0/0
* RT3 Network gigabitEthernet 0/2
* RT-M gigabitEthernet 0/2 <—> RT-3 gigabitEthernet 0/1
* RT4 Network gigabitEthernet 0/0
* RT4 gigabitEthernet 0/1 <—> RT-3 gigabitEthernet 0/0

Addressing:

* RT1 —> 192.168.10.1
* RT1 <—> RT-M, 192.168.70.1
* RT-M <—> RT1, 192.168.70.2
* RT3 —> 192.168.30.1
* RT-M <—> RT3, 192.168.60.2
* RT3 <—> RT-M, 192.168.60.1
* RT4 —> 192.168.40.1
* RT3 <—> RT4, 192.168.50.1
* RT4 <—> RT3, 192.168.50.2

Checking, reload:

* show ip ospf neighbor
* show ip ospf database
* clear ip ospf process

### Router 1 (RT1)

**!general config, IP link**

enable

configure terminal

interface gigabitEthernet 0/1

ip address 192.168.70.1 255.255.255.0

no shutdown

exit

**!enabling OSPF**

router ospf 20

network 192.168.70.0 0.0.0.255 area 0

network 192.168.10.0 0.0.0.255 area 0

exit

do wr

exit

exit

### Router Main (RT-M)

**!general config, IP link**

enable

configure terminal

interface gigabitEthernet 0/0

ip address 192.168.70.2 255.255.255.0

no shutdown

exit

interface gigabitEthernet 0/2

ip address 192.168.60.2 255.255.255.0

no shutdown

exit

**!enabling OSPF**

router ospf 20

network 192.168.70.0 0.0.0.255 area 0

network 192.168.60.0 0.0.0.255 area 0

exit

do wr

exit

exit

### Router 3 (RT3)

**!general config, IP link**

enable

configure terminal

interface gigabitEthernet 0/1

ip address 192.168.60.1 255.255.255.0

no shutdown

exit

interface gigabitEthernet 0/0

ip address 192.168.50.2 255.255.255.0

no shutdown

exit

**!enabling OSPF**

router ospf 20

network 192.168.60.0 0.0.0.255 area 0

network 192.168.30.0 0.0.0.255 area 0

network 192.168.50.0 0.0.0.255 area 0

network 192.168.40.0 0.0.0.255 area 0

exit

do wr

exit

exit

### Router 4 (RT4)

**!general config, IP link**

enable

configure terminal

interface gigabitEthernet 0/1

ip address 192.168.50.1 255.255.255.0

no shutdown

exit

**!enabling OSPF**

router ospf 20

router-id 4.4.4.4

network 192.168.50.0 0.0.0.255 area 0

network 192.168.40.0 0.0.0.255 area 0

exit

do wr

exit

exit

## 11. WAN Protocols: VPN Site-To-Site over IPv4

VPN IPsec (Internet Protocol Security): Creates encrypted connections over the Internet between two networks (site-to-site), protecting the confidentiality and integrity of data.

Compatible hardware:

* Router model No 2911
* Switche model No 2690

“checking VPN Ipsec: look for technology: ipbasek9:permanent and secirityk9:evaluation”

show version

show crypto IPsec sa

### Router 1 (RT1)

**!enabling security technology package**

license boot module c2900 technology-package securityk9

do write

exit

copy run start

reload

enable

configure terminal

crypto isakmp policy 10

encr aes 256

authentication pre-share

group 5

!

crypto isakmp key vpnpass address 192.168.60.1

!

crypto isakmp key vpnpass address 192.168.50.1

!

crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

!

crypto map VPN-MAP 10 ipsec-isakmp

description VPN connection to Branch\_Router

set peer 192.168.60.1

set peer 192.168.50.1

set transform-set VPN-SET

match address 110

!

interface GigabitEthernet0/1

crypto map VPN-MAP

!

end

copy run start

### Router 3 (RT3)

**!enabling security technology package**

license boot module c2900 technology-package securityk9

do write

exit

copy run start

reload

enable

configure terminal

crypto isakmp policy 10

encr aes 256

authentication pre-share

group 5

!

crypto isakmp key vpnpass address 192.168.70.1

!

crypto isakmp key vpnpass address 192.168.50.1

!

crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

!

crypto map VPN-MAP 10 ipsec-isakmp

description VPN connection to Branch\_Router

set peer 192.168.70.1

set peer 192.168.50.1

set transform-set VPN-SET

match address 110

!

interface GigabitEthernet0/1

crypto map VPN-MAP

!

end

copy run start

### Router 4 (RT4)

**!enabling security technology package**

license boot module c2900 technology-package securityk9

do write

exit

copy run start

reload

enable

configure terminal

crypto isakmp policy 10

encr aes 256

authentication pre-share

group 5

!

crypto isakmp key vpnpass address 192.168.60.1

!

crypto isakmp key vpnpass address 192.168.70.1

!

crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

!

crypto map VPN-MAP 10 ipsec-isakmp

description VPN connection to Branch\_Router

set peer 192.168.70.1

set peer 192.168.60.1

set transform-set VPN-SET

match address 110

!

interface GigabitEthernet0/1

crypto map VPN-MAP

!

end

copy run start

## 12. WAN Protocols: VPN Site-To-Site over IPv4

My network doesn't support PPP because the connections are Ethernet. PPP requires serial connections. Additionally, PPP isn't compatible with HSRP. So I'll use the reference network given in class.

Applied on Routers R1, R2, R3 and ISP. Using of CHAP as an automatic authentication method instead of PAP.



**Summary:**

**!setting up Encapsulation Method**

interface <WAN\_to\_target>

encapsulation ppp

!

**!setting up PPP Authentication**

username <Router\_target> secret cisco

interface SALIDA

ppp authentication chap

## Implementation PPP

### R1

interface serial 0/0/0

encapsulation ppp

exit

username R3 secret cisco

interface serial 0/0/0

ppp authentication chap

exit

R2

interface serial 0/0/1

encapsulation ppp

exit

username R3 secret cisco

interface serial 0/0/1

ppp authentication chap

exit

### R3

interface serial 0/0/0

encapsulation ppp

exit

interface serial 0/0/1

encapsulation ppp

exit

interface serial 0/1/0

encapsulation ppp

exit

!second step on R3

username R1 secret cisco

interface serial 0/0/0

ppp authentication chap

exit

!

username R2 secret cisco

interface serial 0/0/1

ppp authentication chap

exit

!

username ISP secret cisco

interface serial 0/1/0

ppp authentication chap

exit

### ISP

interface serial 0/0/0

encapsulation ppp

exit

username R3 secret cisco

interface serial 0/0/0

ppp authentication chap

exit

# Network Security Implementation

## 10. Apply Access Control Lists (ACLS)

Implementing ALC over IPv4 networks.

Checking:

* show access-lists

### Router 1 (RT1)

access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255

access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255

access-list 110 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255

access-list 110 permit ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255

!

copy run start

### Router 3 (RT3)

access-list 110 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255

access-list 110 permit ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255

access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255

access-list 110 permit ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255

!

copy run start

### Router 4 (RT4)

access-list 110 permit ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255

access-list 110 permit ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255

access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255

access-list 110 permit ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255

!

copy run start

## 2. Secure Access Switches By SSH & Telnet

Checking:

* show running-config
* ssh -l administrator <ip\_vlan1>
* telnet <ip\_vlan1>
* service password-encryption

### Switch 1 (sw1)

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.10.96 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw1

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Switch 2 (sw2)

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.10.95 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw2

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Switch 3 (sw3)

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.10.94 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw3

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Switch 4 (sw4)

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.10.93 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw4

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Switch 5 (sw5)

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.10.92 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw5

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Multi-layer Switch 1 (swm1)

Before configure, install AC-POWER-SUPPLY module.

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.10.98 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname swm1

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Multi-layer Switch 2 (swm2)

Before configure, install AC-POWER-SUPPLY module.

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.10.97 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname swm2

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Switch 6 (sw6)

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.30.96 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw6

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Switch 7 (sw7)

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.30.95 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw7

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Switch 8 (sw8)

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.30.94 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw8

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Switch 9

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.30.93 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw9

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Multi-layer Switch 3 (swm3)

Before configure, install AC-POWER-SUPPLY module.

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.30.98 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname swm3

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Multi-layer Switch 4 (swm4)

Before configure, install AC-POWER-SUPPLY module.

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.30.97 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname swm4

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

### Switch 10

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.40.97 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw10

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

## 2. Secure Access Routers By SSH & Telnet

Checking:

* show running-config
* ssh -l administrator <ip\_router>
* telnet <ip\_router>
* service password-encryption

### Router 1 (RT1)

enable

configure terminal

!enabling password

enable password admin

!

!enabling vlan

interface VLAN 1

ip address 192.168.10.96 255.255.255.0

no shutdown

exit

do wr

!enabling password on virtual terminals

service password-encryption

username administrator password cisco

ip domain-name milestones.com

hostname sw1

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

## Routers: RT1, RT2, RT3, RT4, RT-M

Use next configuration on all router on this network:

enable

configure terminal

**!enabling password**

enable password admin

!

**!enabling password on virtual terminals**

service password-encryption

username administrator password cisco

ip domain-name milestones.com

crypto key generate rsa general-keys modulus 1024

!

ip ssh version 2

line vty 5 15

transport input ssh

login local

exit

!

line vty 0 4

transport input telnet

password cisco

login

!

exit

!

do wr

!

exit

!

# Legal & security: Policies and Procedures

ABC Enterprises adopts security technologies to ensure data protection. The company's policies are outlined below.

## 1. Service Password Encryption

Policy to prevent access to plain-text passwords in network devices. In compliance with standard ISO/IEC 27001.

ISO/IEC 27001 – to safeguarding of authentication credentials and sensitive information stored in system configurations.

## 2. Mandatory Login Password

Policy on all network devices that requires a login password for any access to routers or switches. In compliance with NIST SP 800-53 (IA-2).

NIST SP 800-53 (IA-2) – apply authentication mechanisms are mandatory to verify user identity prior to access to network infrastructure.

## 3. VPN Site-to-Site

Policy implements IPSec to protect data in transit between different company branches over internet. In compliance with NIST SP 800-77.

NIST SP 800-77 – provides guidance for the secure deployment of IPsec VPNs in enterprise environments.

## 4. Access Control Lists (ACLs)

Policy to filter traffic and control access between subnets, enhance internal network security. In compliance with ISO/IEC 27002 (s13)

ISO/IEC 27002 – control and restrics network access to authorized communications only.

## 5. Secure Remote Access to infrastructure

Policy to protect remote access by Telnet and SSH to network devices using password-protected and encrypted. In compliance with This configuration aligns with: NIST SP 800-5.

NIST SP 800-52 – secure protocols for administrative access and discourages the use of unencrypted communication channels.

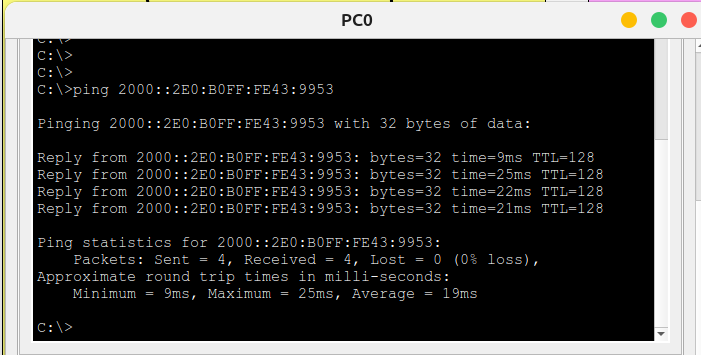
# Troubleshooting & Testing

## 1. Testing LAN Connectivity (IPv4/IPv6)

# Sydney Branch

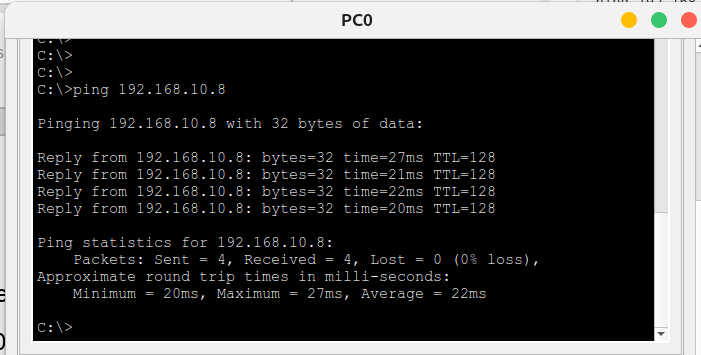


* Connectivity between Commercial and Admin over IPv6  
  PC0 LAPTOP0



* Connectivity between Commercial and Admin over IPv4

PC0 LAPTOP0



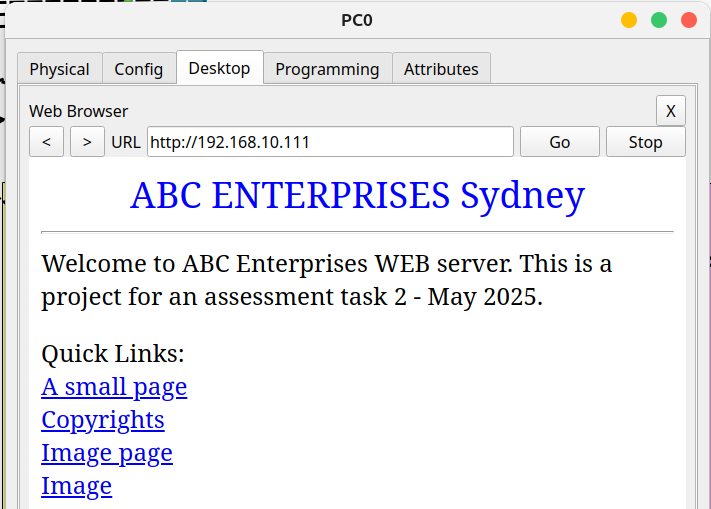
* Connectivity between Commercial and Comms over IPv6

WEB PC0



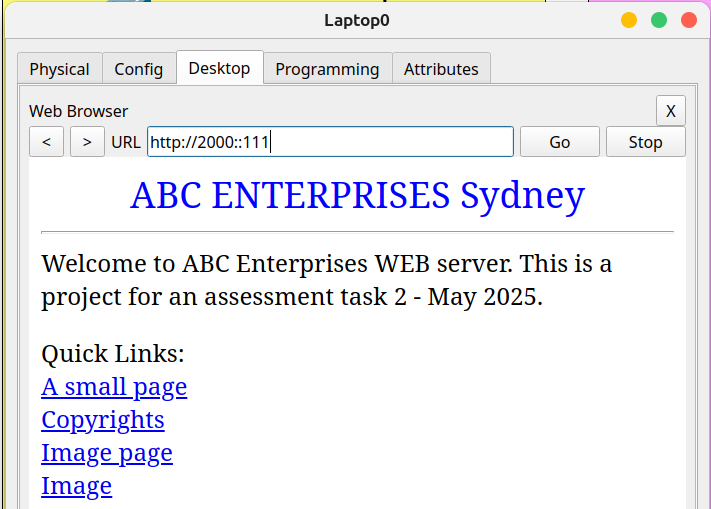
* Connectivity between Commercial and Comms over IPv4

WEB PC0



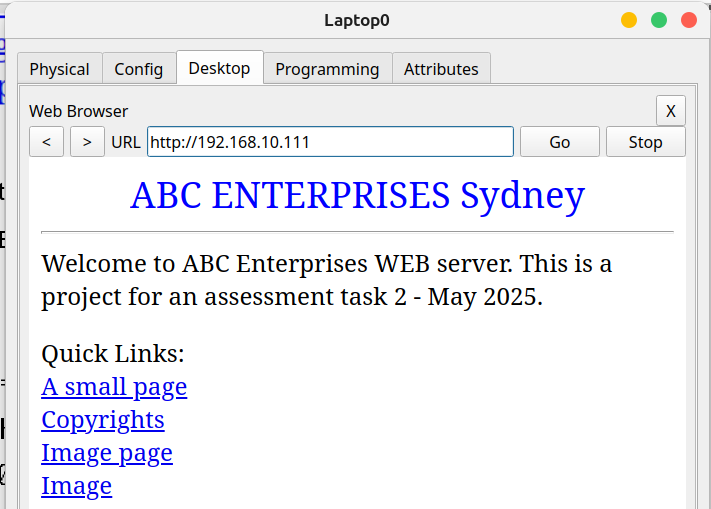
* Connectivity between Admin and Comms over IPv6

LAPTOP0 WEB

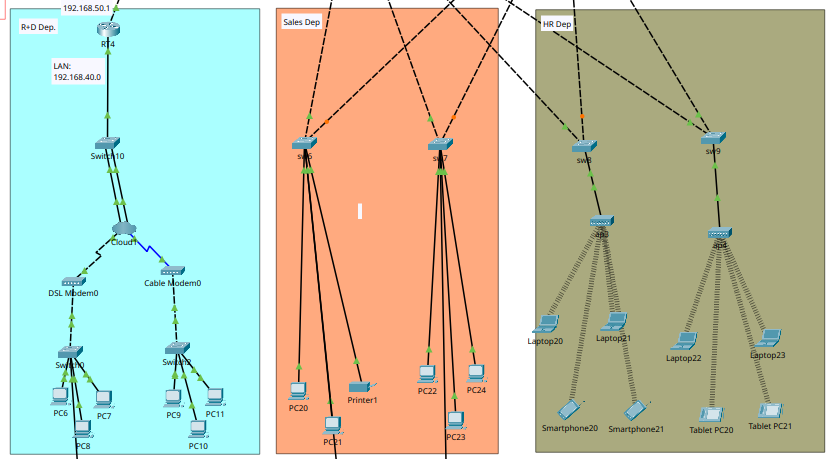


* Connectivity between Admin and Comms over IPv4

LAPTOP0 WEB

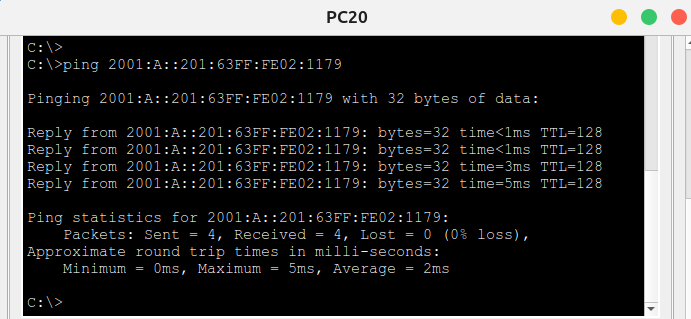


# Brisbane Branch



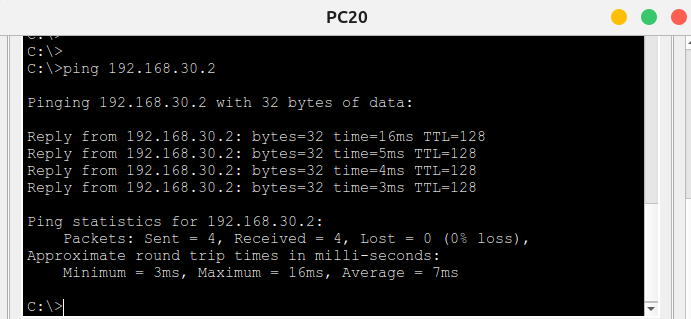
* Connectivity between Sales and HR over IPv6

PC20 LAPTOP20



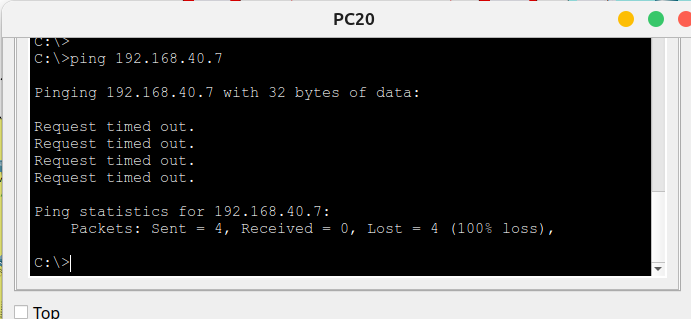
* Connectivity between Sales and HR over IPv4

PC20 LAPTOP20



* Connectivity between Sales and R+D over IPv4

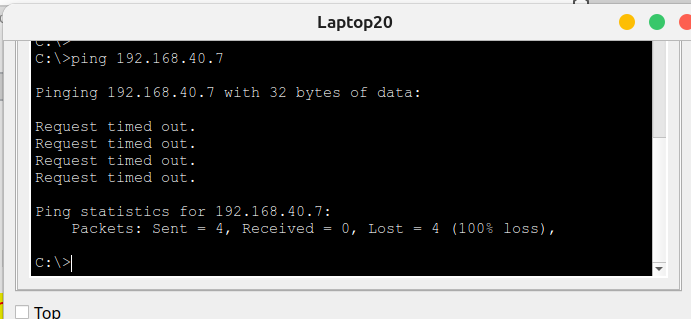
PC20 PC6 – After implement VPN this connection is no longer available, I could not fixed it.



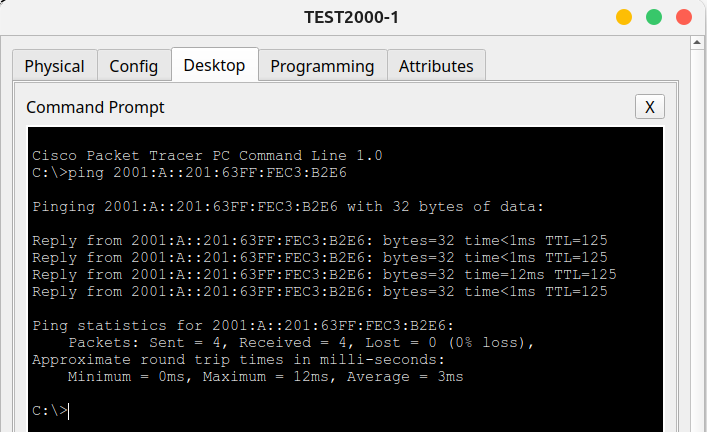
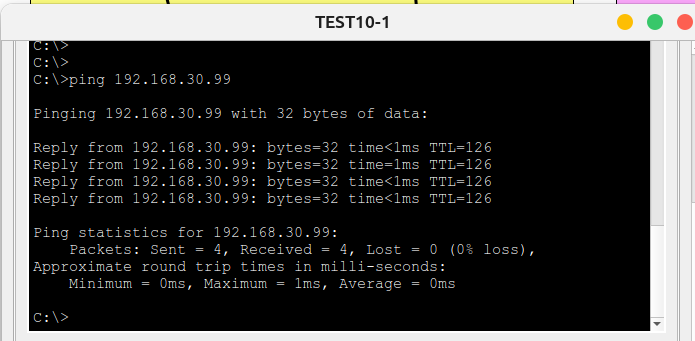
* Connectivity between HR and R+D over IPv4

LAPTOP20 PC6 - After implement VPN this connection is no longer available, I could not fixed it.

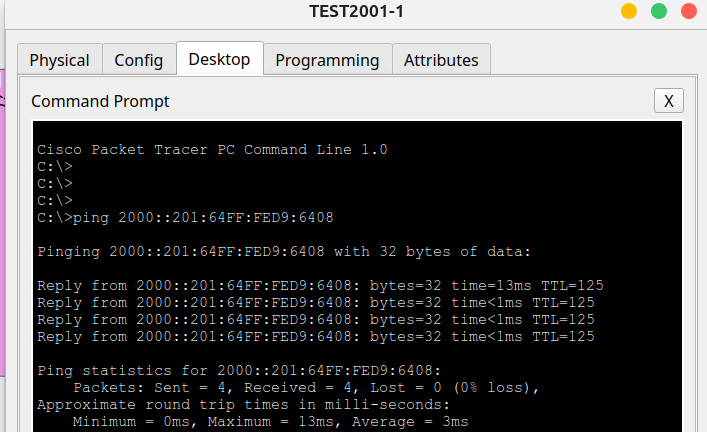
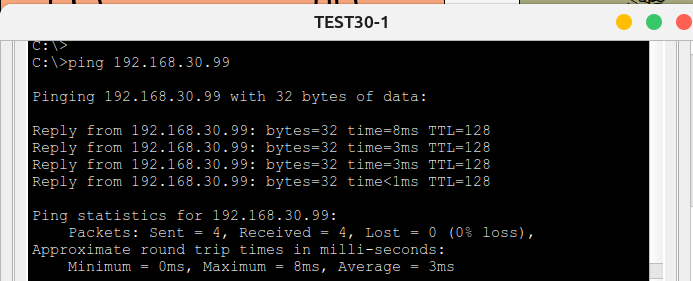
## 2. Testing WAN Connectivity (IPv4/IPv6)



* Connectivity between Sydney Branch and Brisbane Branch



* Connectivity between Brisbane Branch and Sydney Branch



**Notes:**

==================================================================

Sydney Branch ===================================================

PC0 = 2000::201:97FF:FEB1:9D70

PC0 = 192.168.10.2

LAPTOP0 = 2000::2E0:B0FF:FE43:9953

LAPTOP0 = 192.168.10.8

WEB = 2000::111

WEB = 192.168.10.111

==================================================================

Brisbane Branch =================================================

PC20 = 2001:A::201:63FF:FE02:1179

PC20 = 192.168.30.2

LAPTOP20 = 2001:A::260:70FF:FE99:235C

LAPTOP20 = 192.168.30.9

PC6 ----------------

PC6 = 192.168.40.7

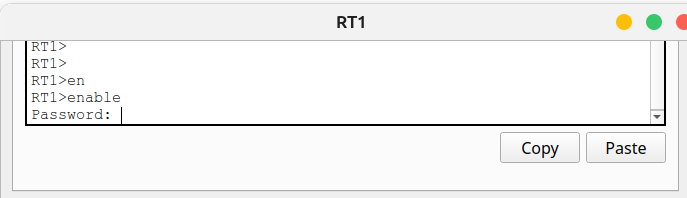
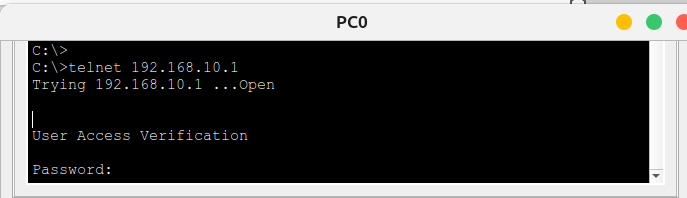
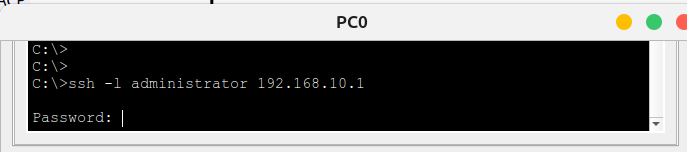
==================================================================

## 3. Testing Secure Access SSH & Telnet - Local

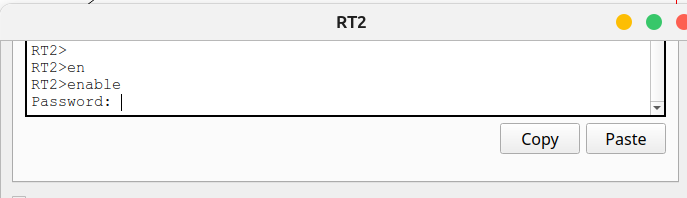
Commands:

SSH = ssh –l administrator <ip>  
Telnet = telnet <ip>

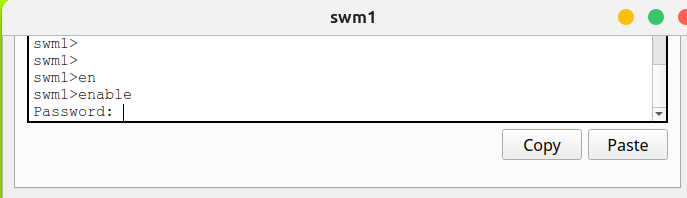
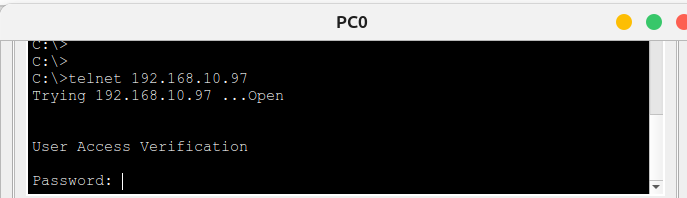
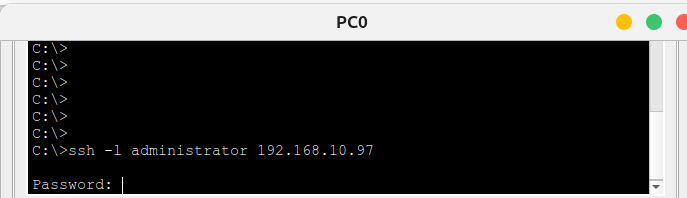
* RT1 192.168.10.1



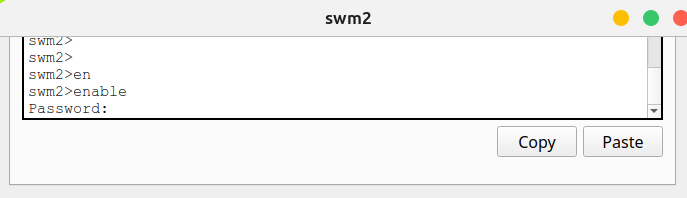
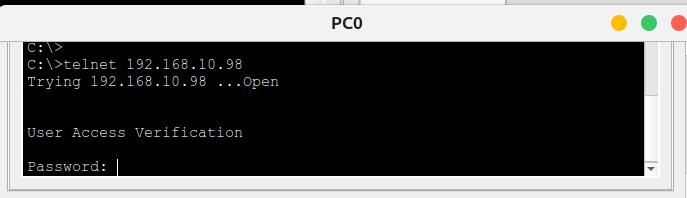
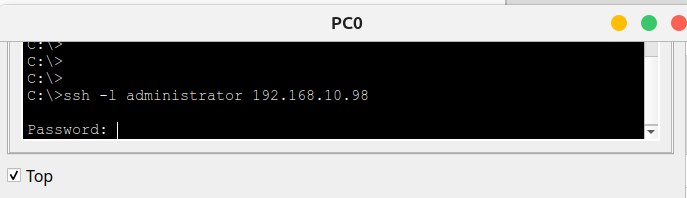
* RT2 2000::3



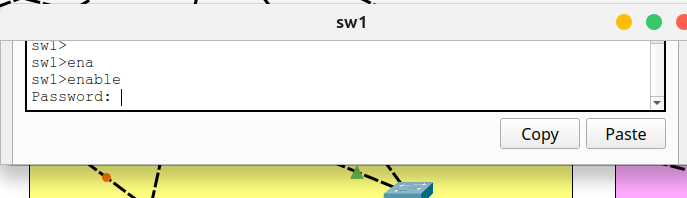
* swm1 VLAN1:192.168.10.97



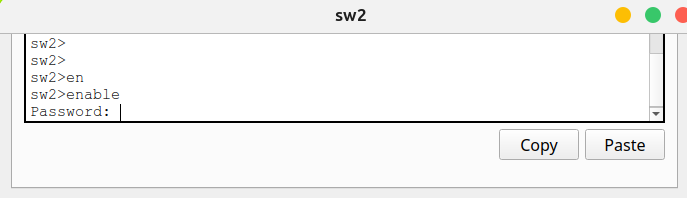
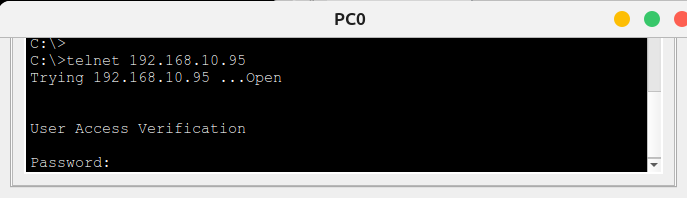
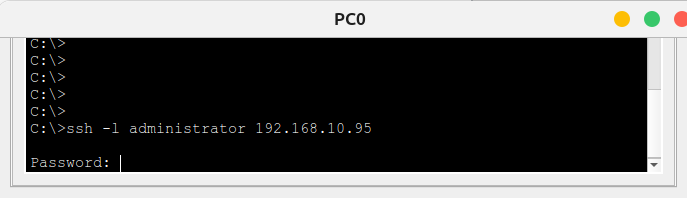
* swm2 VLAN1:192.168.10.98



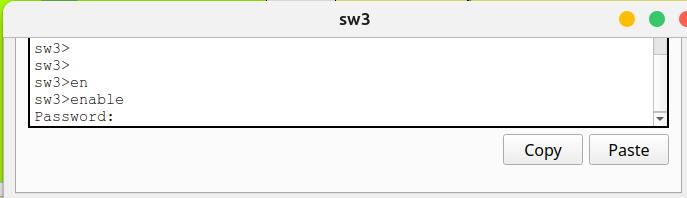
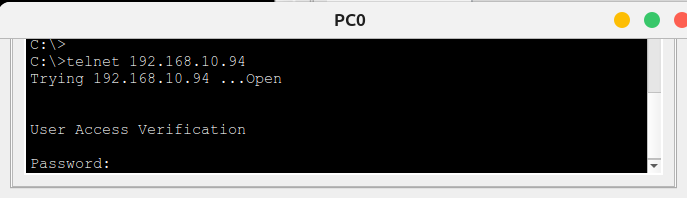
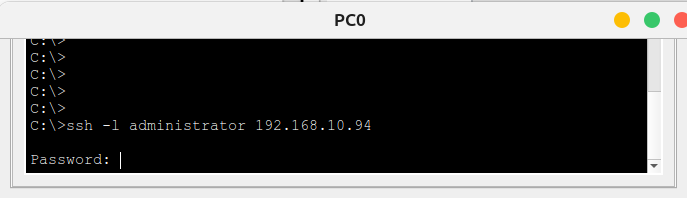
* sw1 VLAN1:192.168.10.96



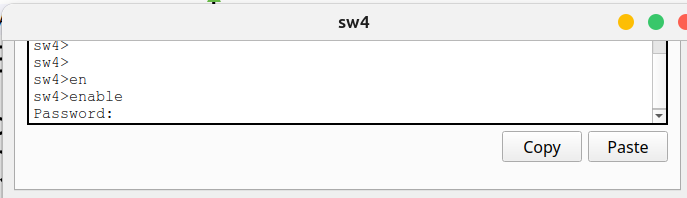
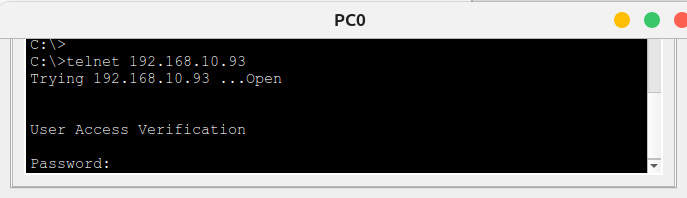
* sw2 VLAN1:192.168.10.95



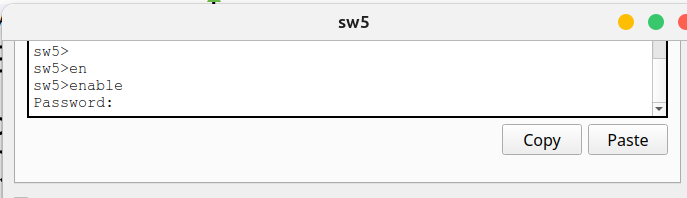
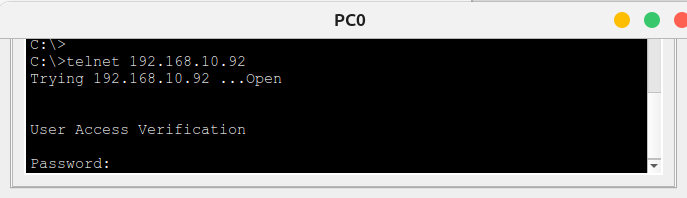
* sw3 VLAN1:192.168.10.94



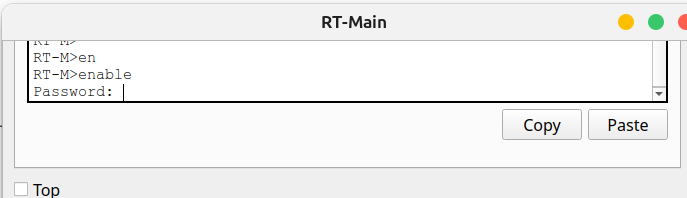
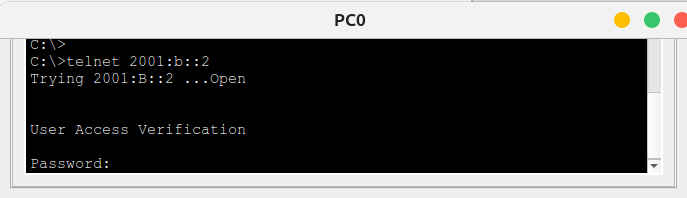
* sw4 VLAN1:192.168.10.93



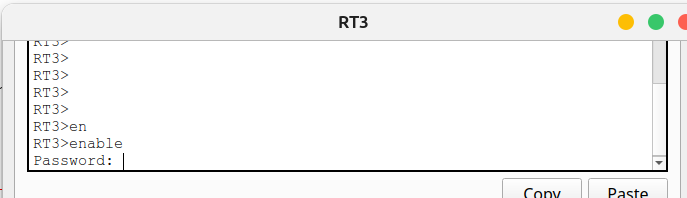
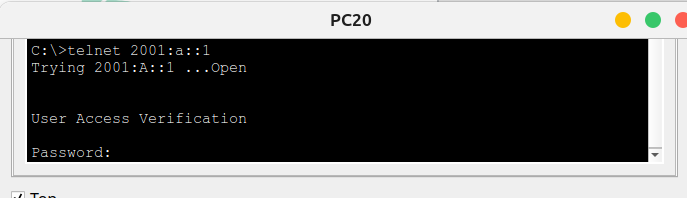
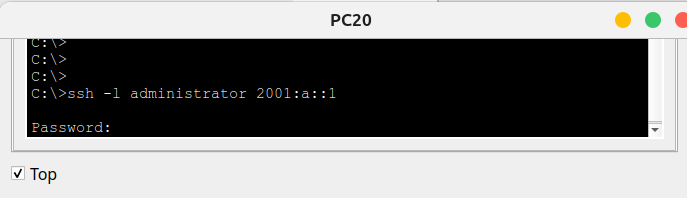
* sw5 VLAN1:192.168.10.92



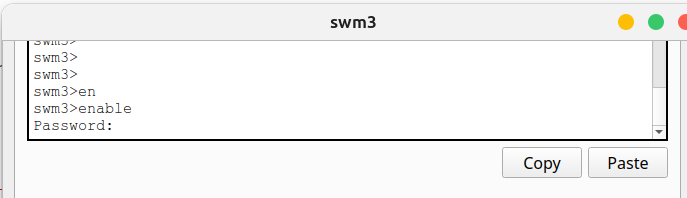
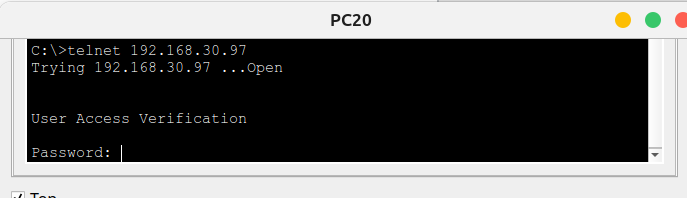
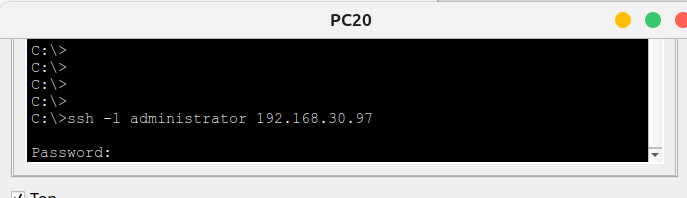
* RT-M 2001:b::2



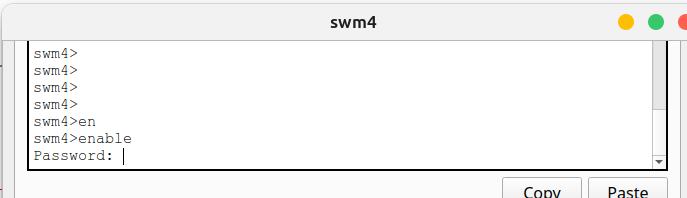
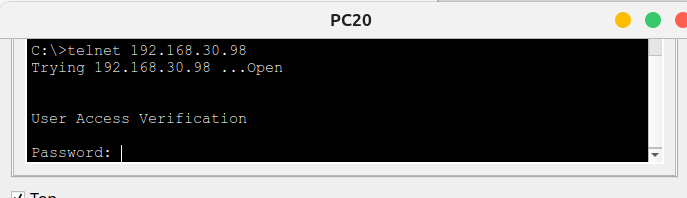
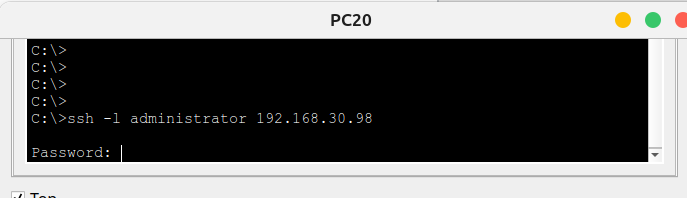
* RT3 2001:a::1



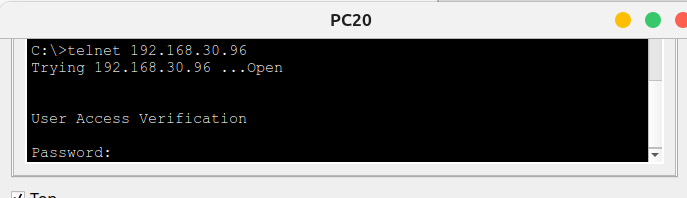
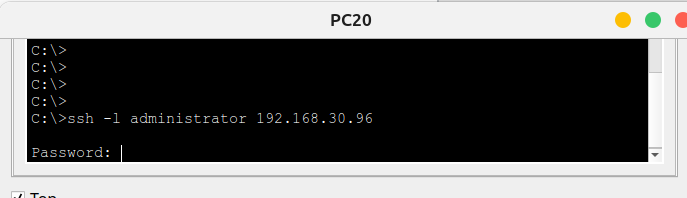
* swm3 VLAN1:192.168.30.97



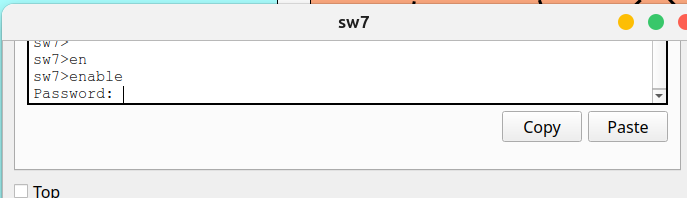
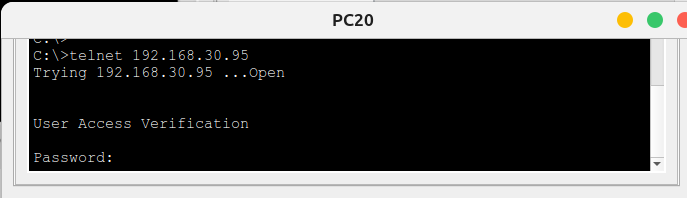
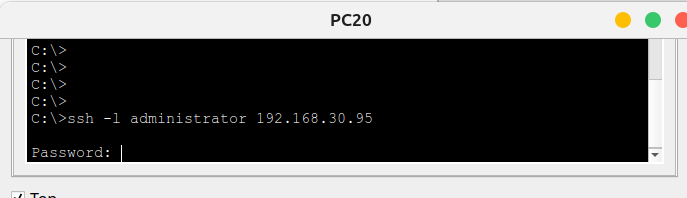
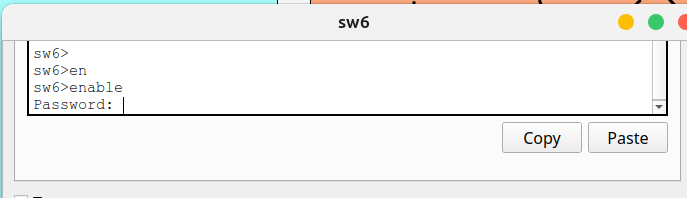
* swm4 VLAN1:192.168.30.98



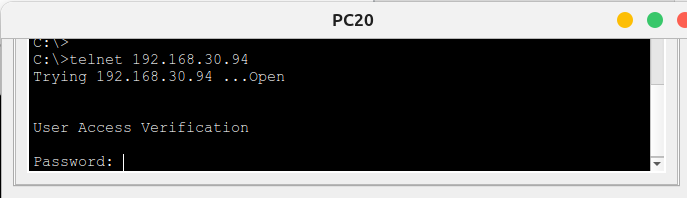
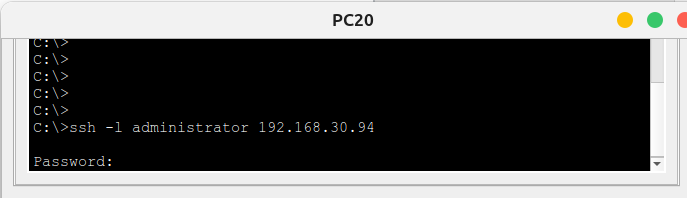
* sw6 VLAN1:192.168.30.96



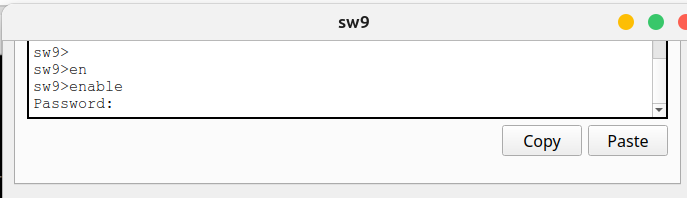
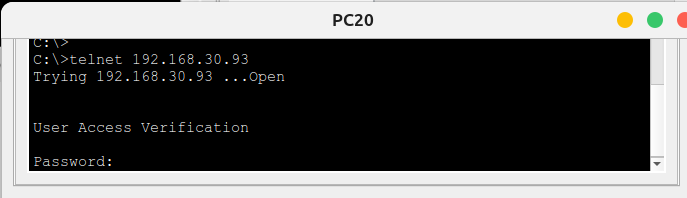
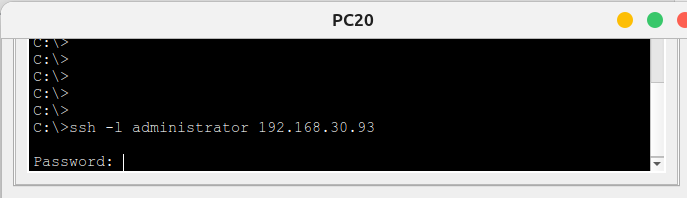
sw7 VLAN1:192.168.30.95



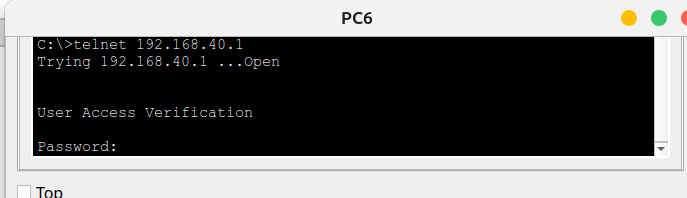
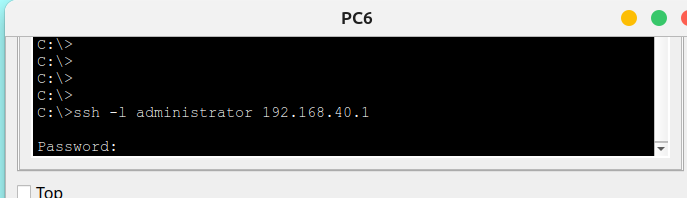
* sw8 VLAN1:192.168.30.94



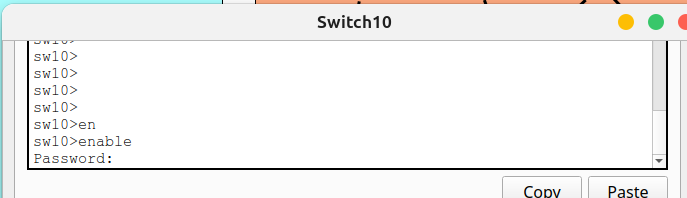
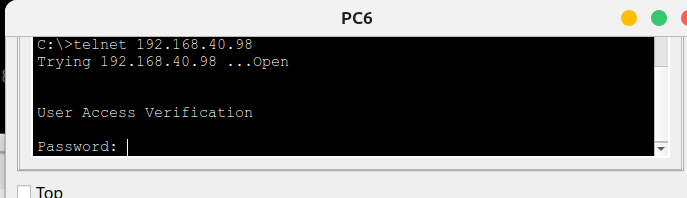
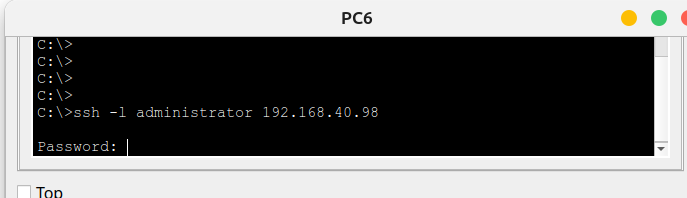
* sw9 VLAN1:192.168.30.93



* RT4 192.168.40.1



* sw10 VLAN1:192.168.40.98



**Notes:**

=========================================================

RT1 192.168.10.1

RT2 2000::3

swm1 VLAN1:192.168.10.97

swm2 VLAN1:192.168.10.98

sw1 VLAN1:192.168.10.96

sw2 VLAN1:192.168.10.95

sw3 VLAN1:192.168.10.94

sw4 VLAN1:192.168.10.93

sw5 VLAN1:192.168.10.92

RT-M

2001:b::2

RT3 2001:a::1

RT4 192.168.40.1

swm3 VLAN1:192.168.30.97

swm4 VLAN1:192.168.30.98

sw6 VLAN1:192.168.30.96

sw7 VLAN1:192.168.30.95

sw8 VLAN1:192.168.30.94

sw9 VLAN1:192.168.30.93

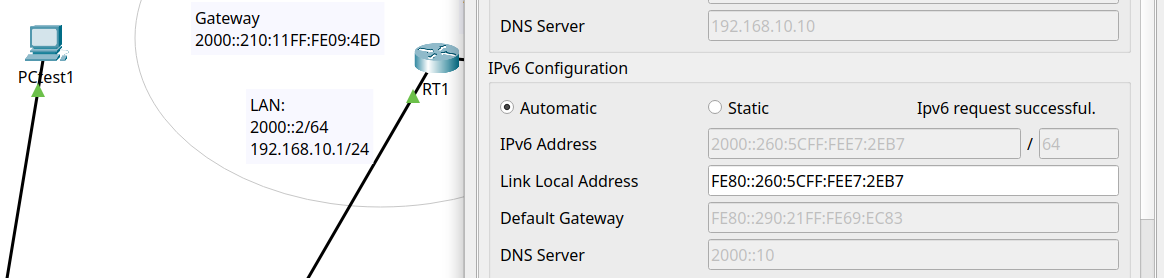
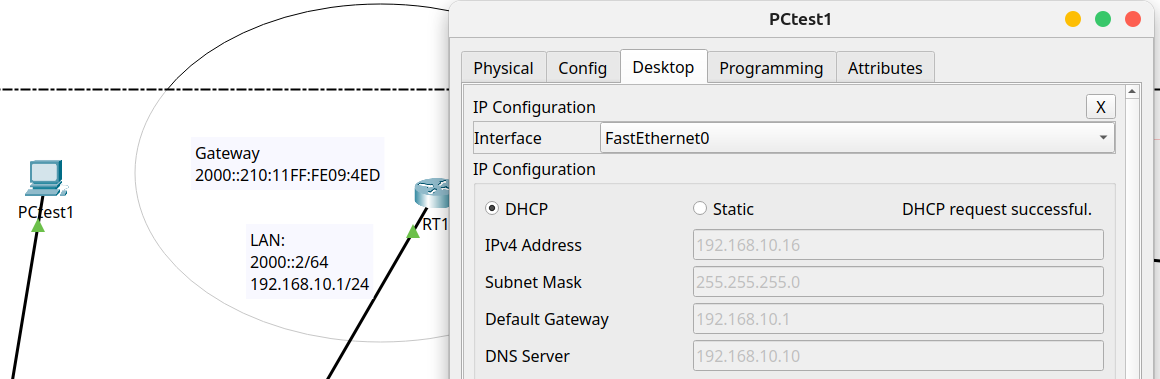
sw10 VLAN1:192.168.40.92

=========================================================

## 4. Testing DHCP/DHCPv6 (IPv4/IPv6)

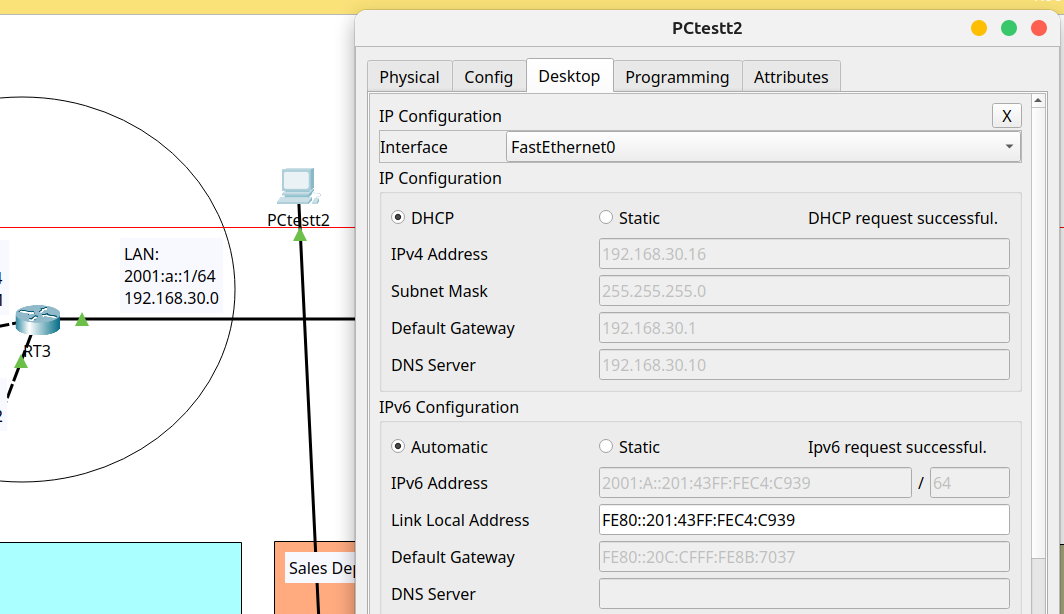
* RT1

New PC configured to DHCP and IPv6 Auto



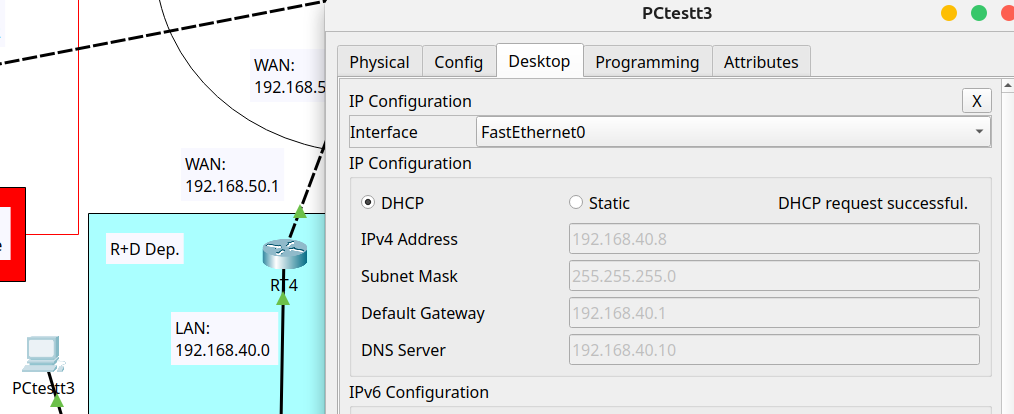
* RT3

New PC configured to DHCP and IPv6 Auto



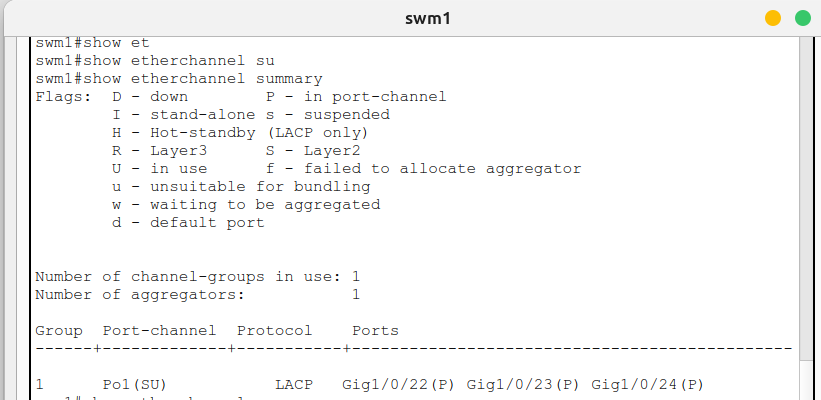
* RT4

New PC configured to DHCP

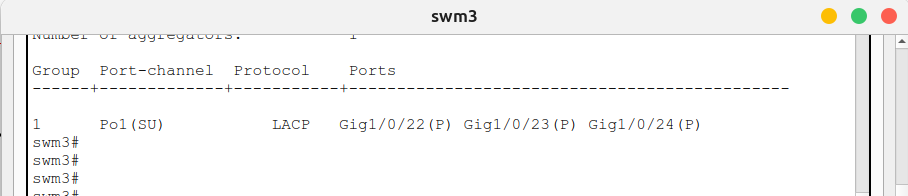


## 5. Testing LACP (IPv6)

* Summary port-channel Sydney Branch

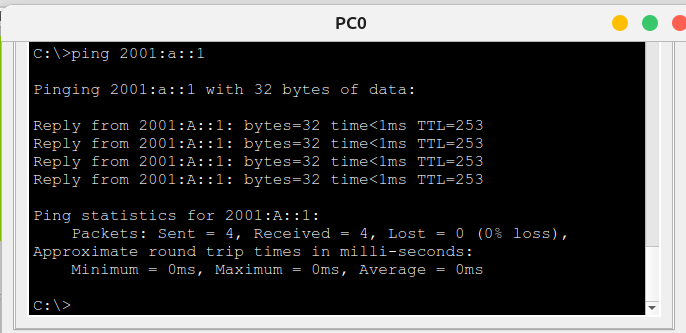
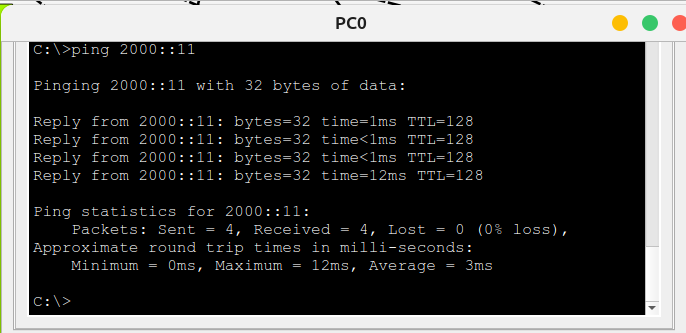
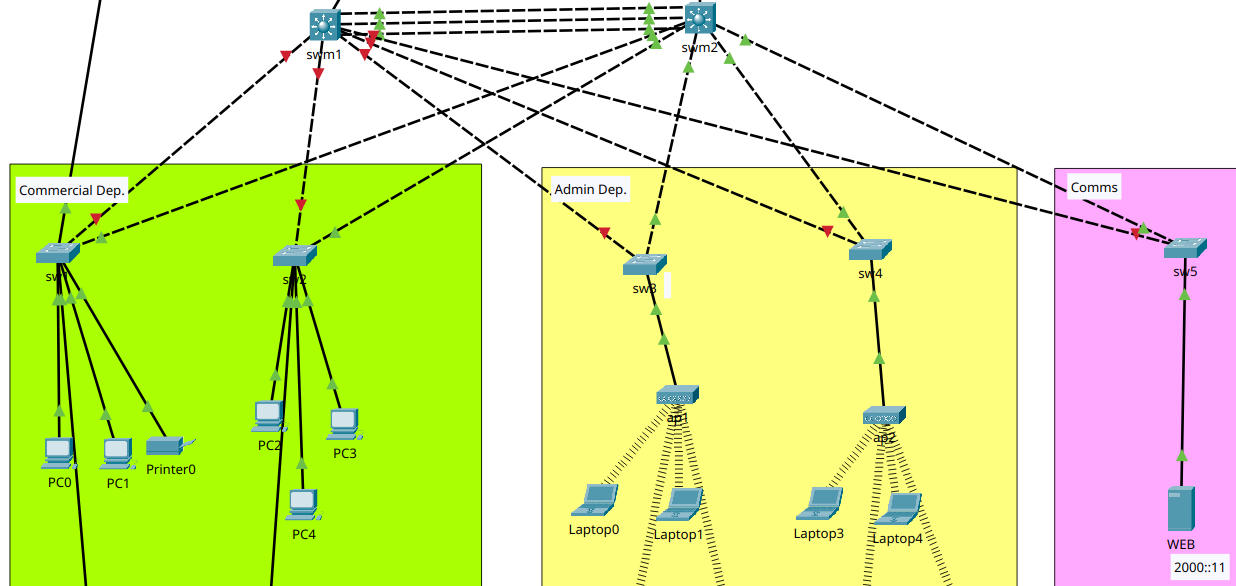


* Summary port-channel Bisbane Branche



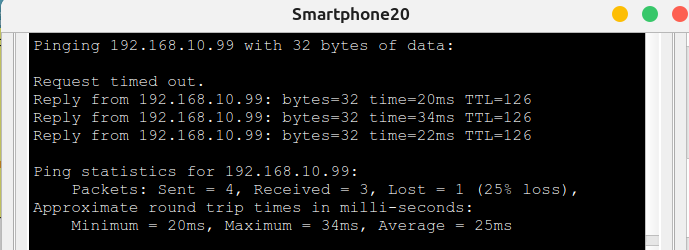
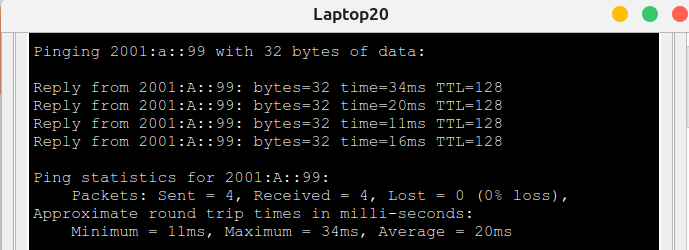
* Testing LACP on Sydney Branch

All connections from swm1 to all local devices was turned off to test redundancy from swm2.



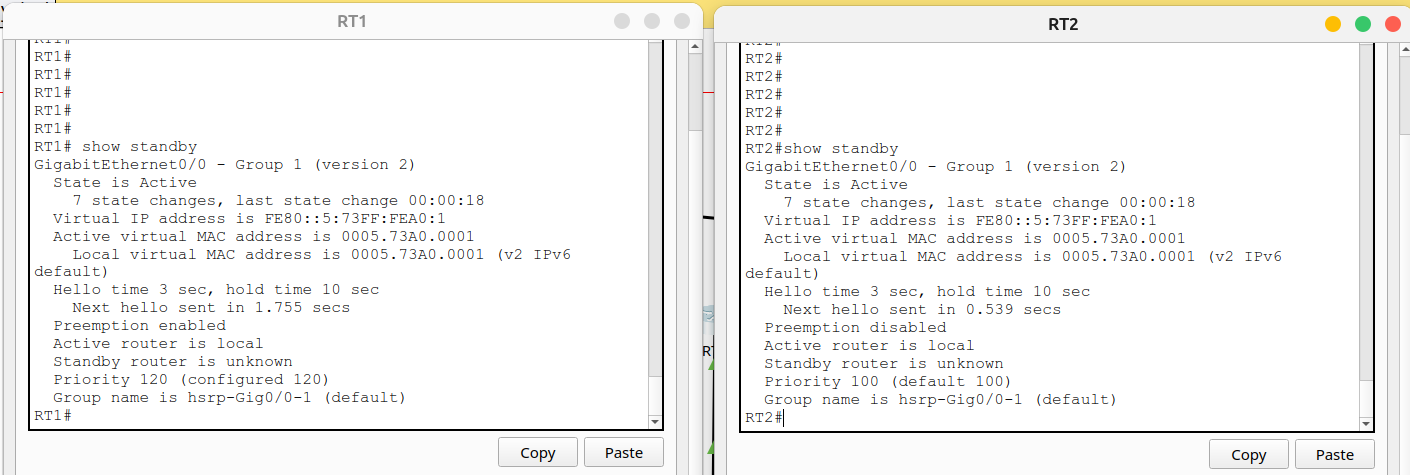
* Testing LACP on Brisbane Branche

All connections from swm3 to all local devices was turned off to test redundancy from swm4.

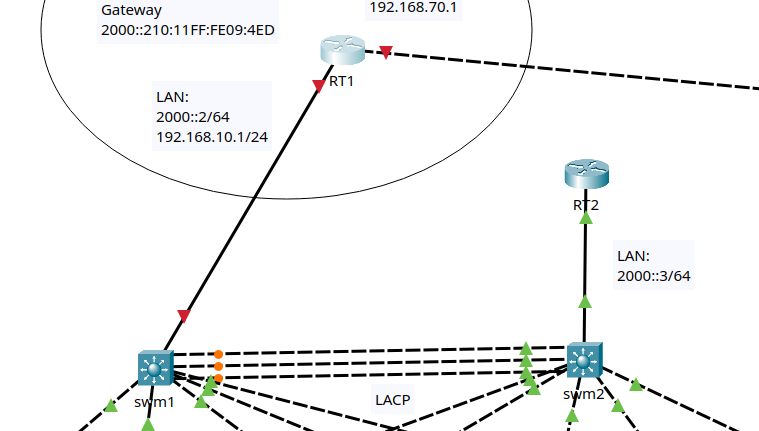


## 6. Testing HSRPv2 (IPv6)

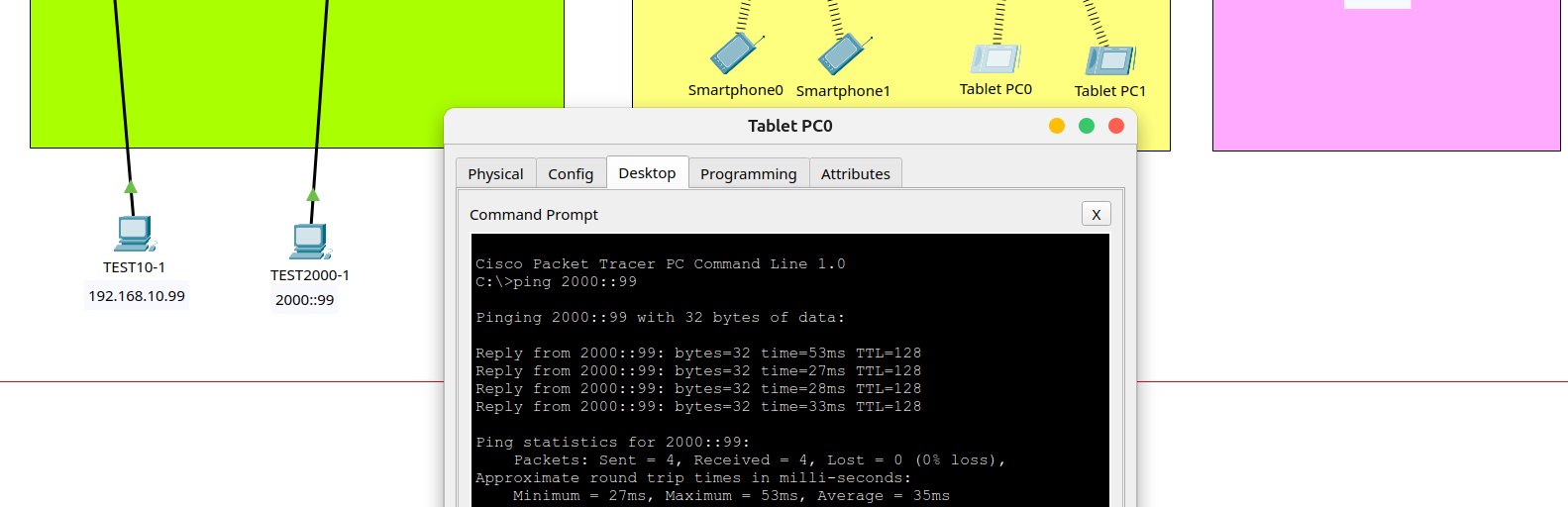
RT1 is running as a primary (priority 120) and RT2 as a secondary (priority 100).



The primary router will be turned off to verify network behaviour.



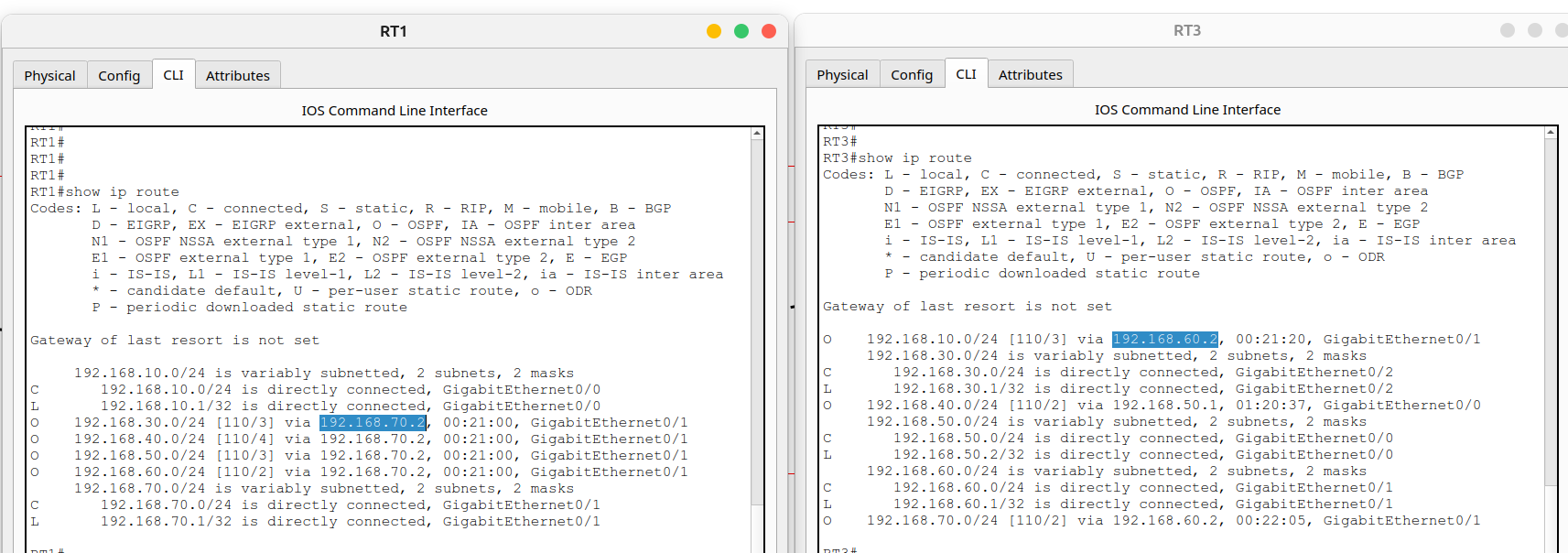
Testing local connection:



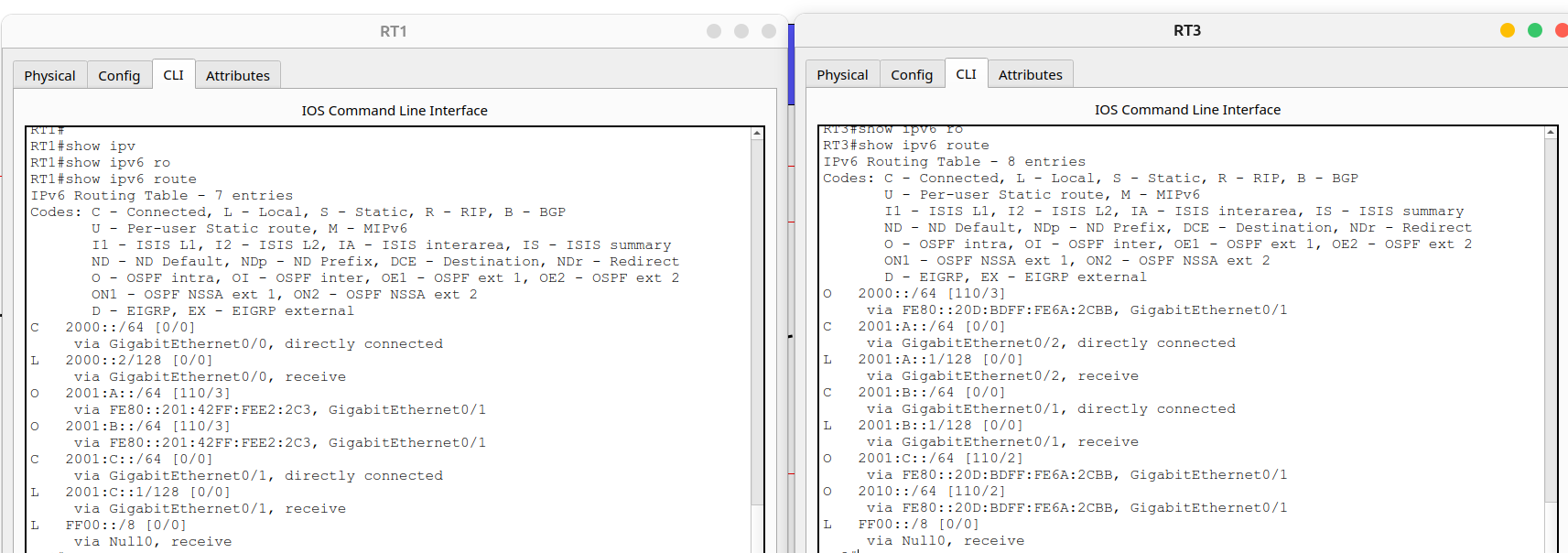
## 7. Testing OSPF/OSPFv3 (IPv4/IPv6)

Routes between devices are proved by OSPF and OSPFv3.

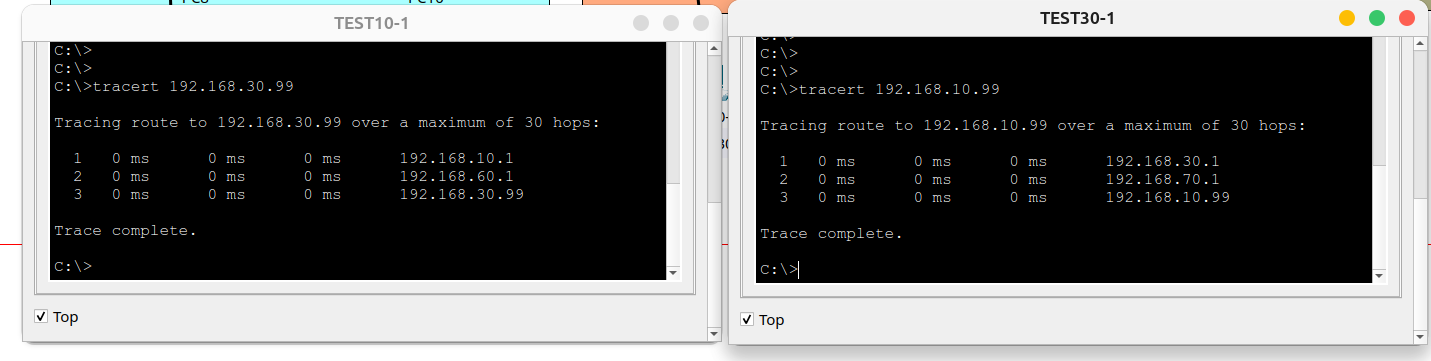
**Communication via WAN interfaces by OSPF**



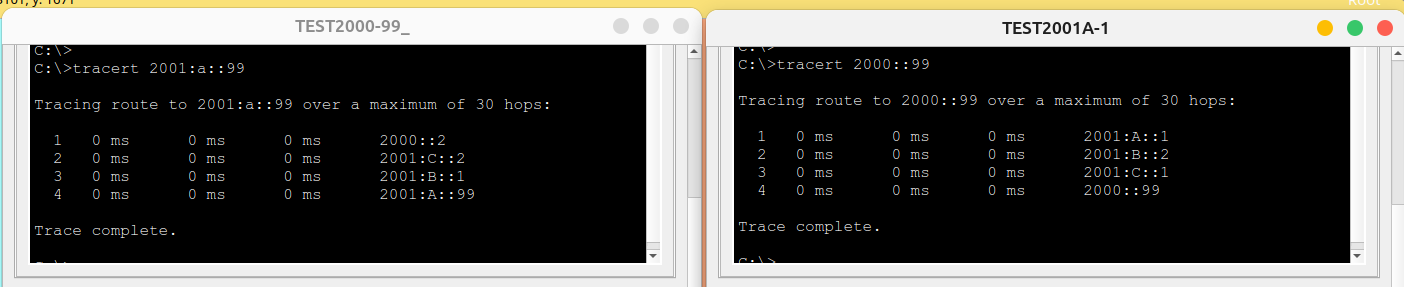
**Communication via WAN interfaces by OSPFv3**



* Bidirectional connectivity testing between Sydney Branch and Brisbane Branch over IPv4

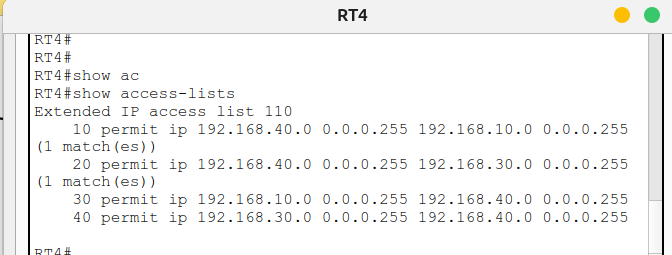
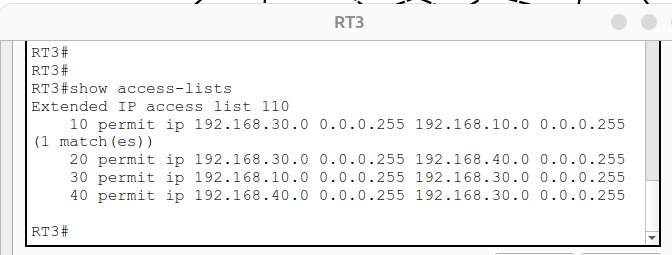
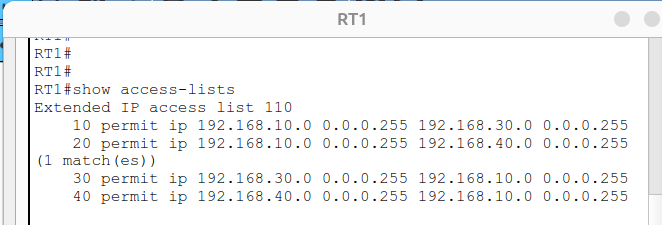


* Bidirectional connectivity testing between Sydney Branch and Brisbane Branch over IPv6

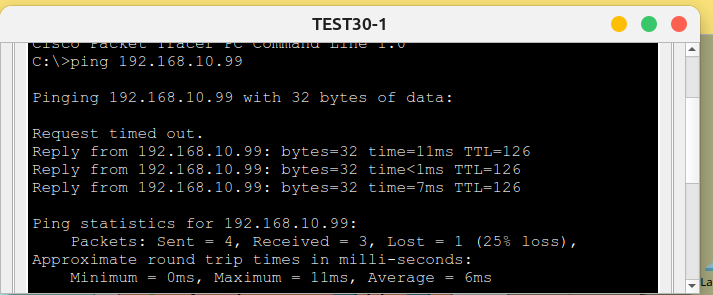


## 8. Testing ACL (IPv4)

**Current Configuration:**



* Test current connectivity from PC-Test (Brisbane IPv4) to PC-Test (Sydney IPv4)



* Test deny connectivity from PC-Test (Brisbane IPv4) to PC-Test (Sydney IPv4)

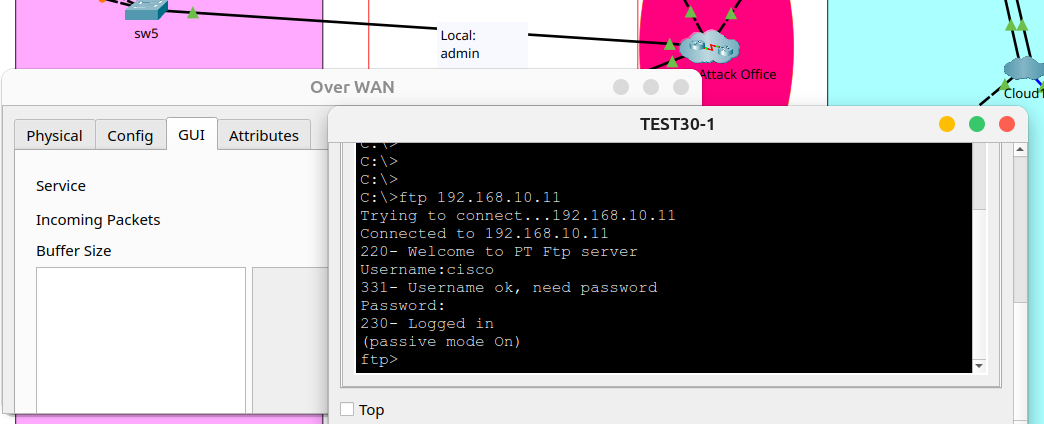
Rule changed on R1 to deny traffic from 192.168.10.99:



## 9. Testing VPN Site-To-Site (IPv4)

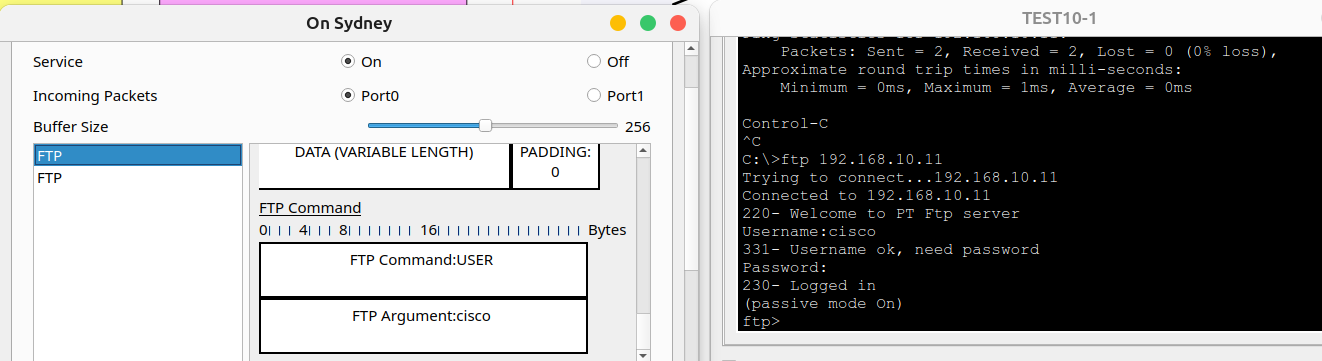
* Internet connection intercepted by a criminal sniffer (secure by VPN tunnel)

**FTP connection from PC on Brisbane Branch to Server on Sydney**



* Local connection intercepted by a criminal sniffer (no secure Lan connection)

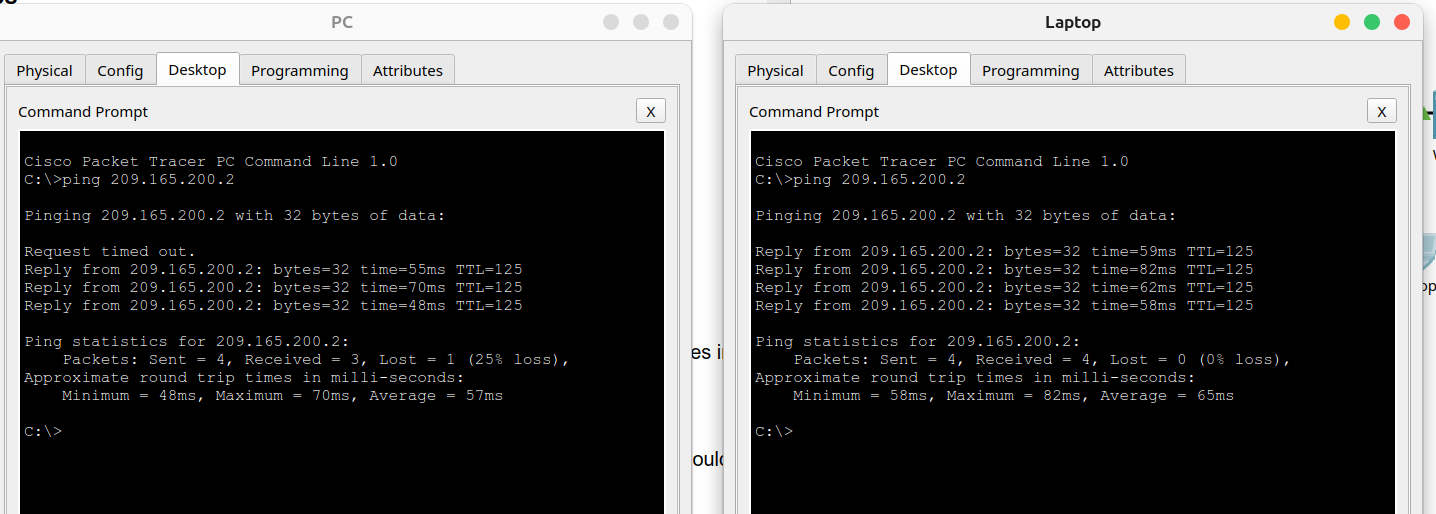
**FTP connection from PC on Sydney Local Network**



## 10. Testing Encapsulation PPP (IPv4)

Applied on Routers R1, R2, R3 and ISP. Using of CHAP as an automatic authentication method instead of PAP.

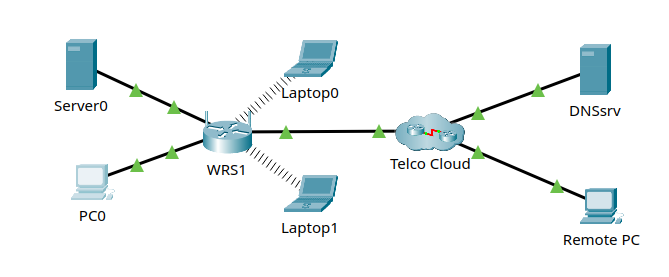
* Testing connection from PC and Laptop to Web



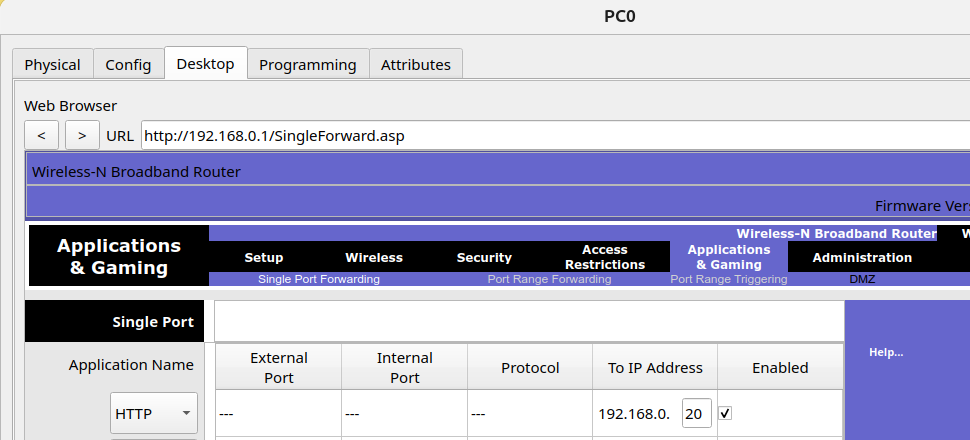
11. Testing Firewall and Single-port

Firewall and single-port tests were performed on the file submitted in class.

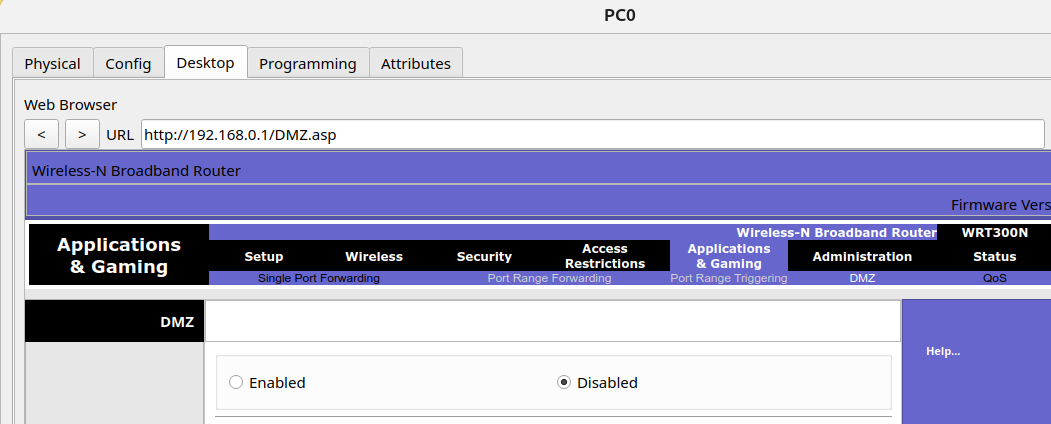
Network:



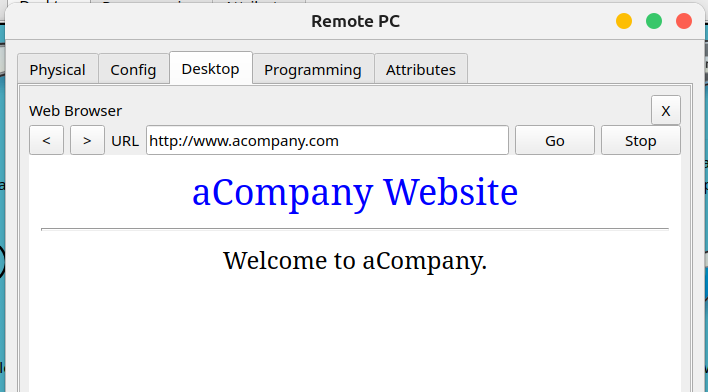
**Configuration – Single-Port enabled:**



Configuration – DMZ disabled:



* Testing connection from Remote PC to WEB Server



# Summary Technologies & Protocols

**DHCP (Dynamic Host Configuration Protocol):**

Automatically assigns IP, gateway, and DNS addresses to devices on the network

**LACP (Link Aggregation Control Protocol):**

Combines several physical links to form a single logical link for the purpose of increasing bandwidth also providing redundancy when one of the switches fails.

**HSRP (Hot Standby Router Protocol):**

Provides redundancy. If the primary router fails, another router automatically takes over, ensuring service continuity.

**OSPF (Open Shortest Path First):**

Dynamic routing that allows the calculation of the most efficient route to send packets in a network.

**ACLs (Access Control Lists):**

Rules applied to allow or deny traffic. They are used to filter traffic and improve security.

**VPN IPsec (Internet Protocol Security):**

Creates secure (encrypted) connections over the Internet between two networks (site-to-site), protecting data confidentiality and integrity.

**PPP Authentication (Point-to-Point Protocol Authentication):**

Responsible for verifying devices attempting to establish a point-to-point connection. Use of CHAP as an automatic authentication method instead of PAP.

# Bibliography

* Network System: [Gurutech Networking Training - Secure Network Training](https://www.youtube.com/watch?v=Cbv95OxT1FM)
* DHCPv6 Router:  [Gurutech Networking Training - DHCPv6](https://www.youtube.com/watch?v=HQbQuXxqXSo)
* DHCPv6 stateless-stateful: [ShefferKimanzi - DCHP v6 configuration](https://computernetworking747640215.wordpress.com/2019/11/05/configuring-dhcpv6-both-stateless-and-stateful-in-packet-tracer/)
* LACP: [ITExamAnswers.net - Configure EtherChannel](https://itexamanswers.net/6-2-4-packet-tracer-configure-etherchannel-instructions-answer.html) l
* HRSP v2 IPv6: [Packet Tracer Network - HSRP Configuration](https://www.packettracernetwork.com/tutorials/hsrp-configuration-new.html)
* IPCisco.com: [ADSL IPv6](https://ipcisco.com/lesson/ipv6-configuration-on-cisco-packet-tracer/)
* ACLs: [Packet Tracer Network - ACLs](https://www.packettracernetwork.com/tutorials/packet-tracer-acls.html)
* OSPFv3: [Networking Academy - IPv6 OSPFv3](https://www.youtube.com/watch?v=tleCK9KpiMY)
* OSPf: [Computer Networking - OSPF](https://computernetworking747640215.wordpress.com/2018/05/24/ospf-configuration-in-packet-tracer/)
* VPN IPsec tunnel (site-to-site): [Abdullah Irfan, Medium, VPN tunnel](https://dingavinga.medium.com/setting-up-site-to-site-ipsec-on-cisco-packet-tracer-1349890ff3fb)
* VPN site-to-site, IPsec: [Gurutech Networking Training - VPN IPsec](https://www.youtube.com/watch?v=CsAROSbZF-Y)
* SSH:  [Sheffer Kimanzi, Configuring ssh](https://computernetworking747640215.wordpress.com/2018/07/05/secure-shell-ssh-configuration-on-a-switch-and-router-in-packet-tracer/)
* Telnet:  [Sheffer Kimanzi, Configuring telnet](https://computernetworking747640215.wordpress.com/2018/07/05/configuring-telnet-on-a-switch-and-a-router-in-packet-tracer/)