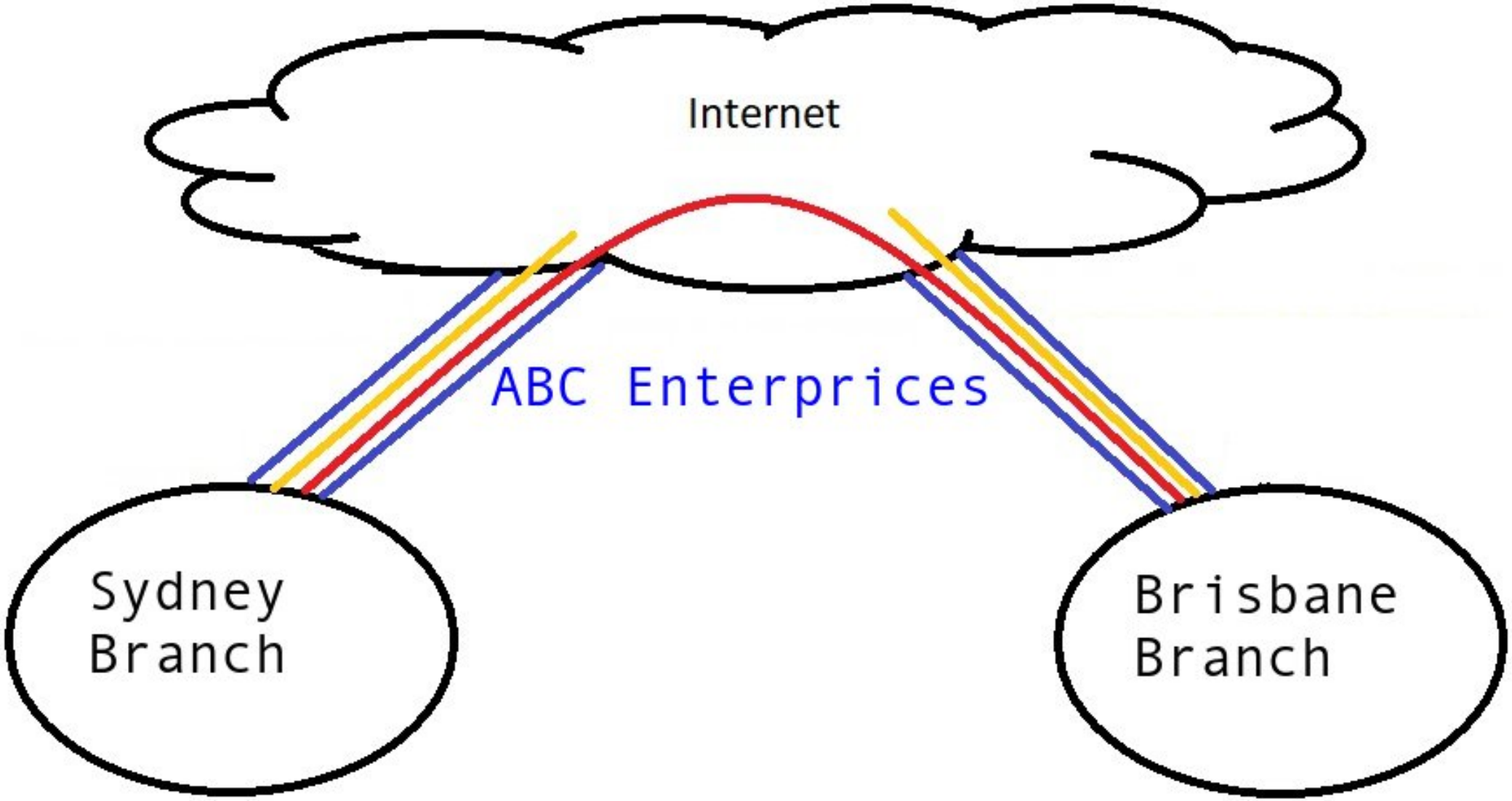
ICTNWK541 Assessment

Assessment Task 2: Project Portfolio

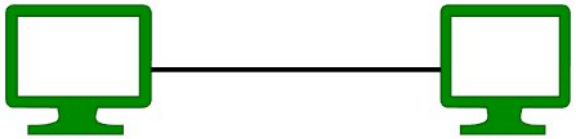
Manuel Sergio Perez Espitia

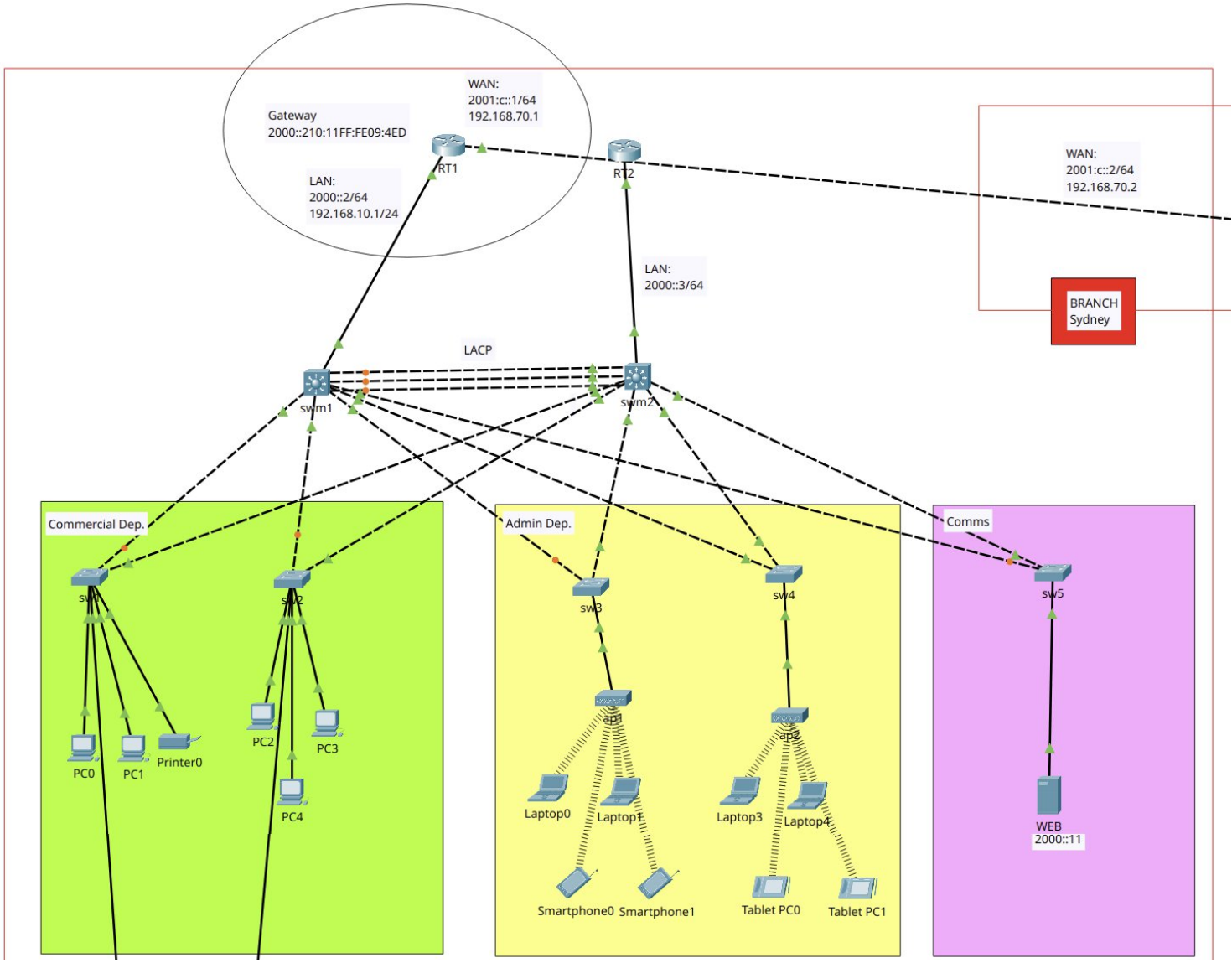

Internet
ABC Enterprices
Sydney
Branch
Brisbane
Branch

We are the network engineer responsible for implementing the required WAN connectivity for ABC Enterprises.

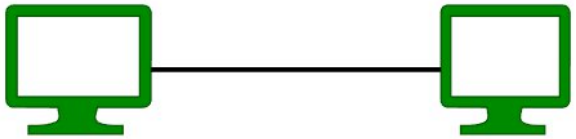
ABC Enterprises wants to improve its network due to old infrastructure, security and reliability WAN connectivity between Sydney Branch and Brisbane Branch.

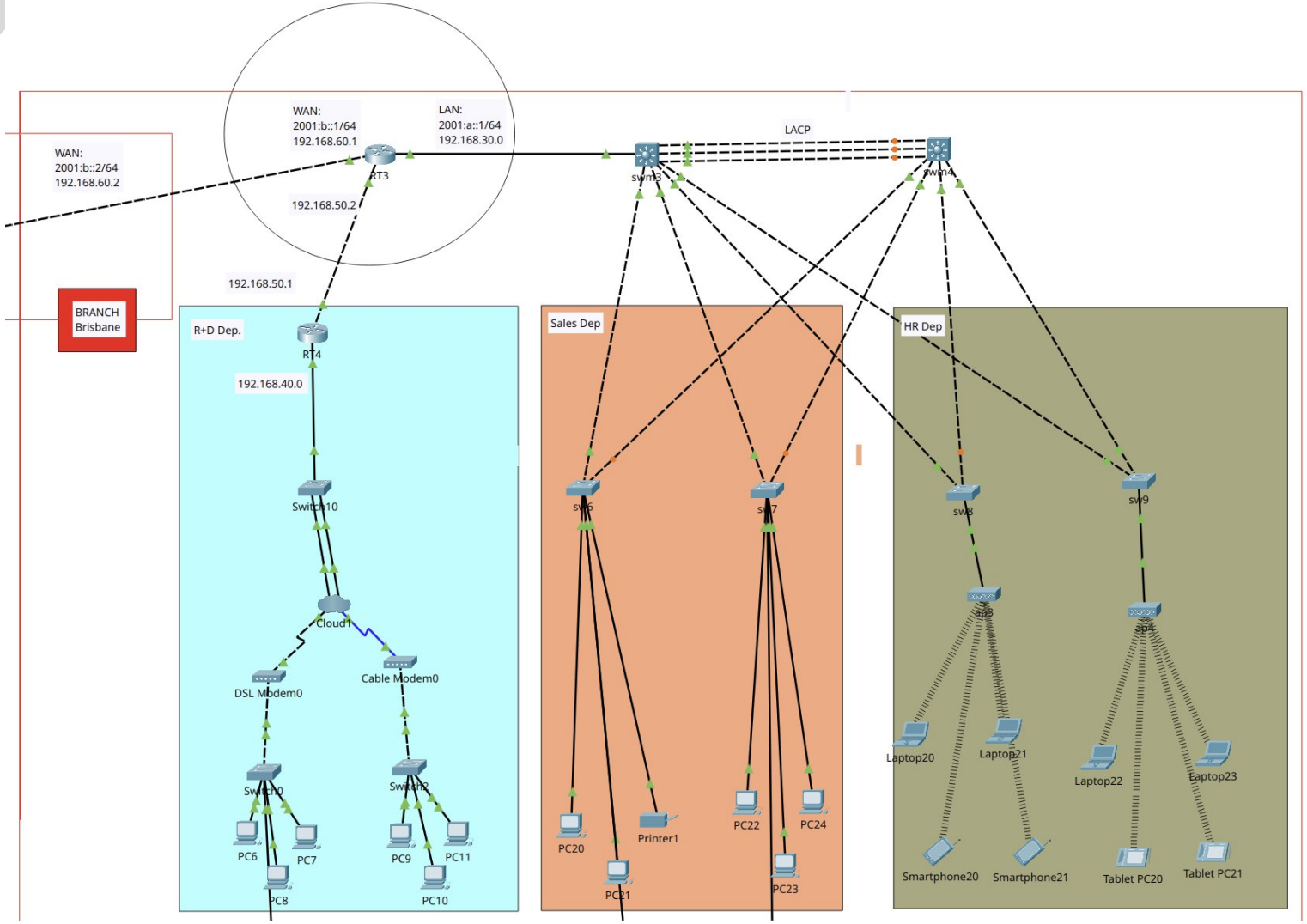
Sydney Branch





Brisbane Branch





Simulation Software & Tools

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

Network Details

Sydney Branch

Type: LAN/WAN

Topology: Dual-Star high availability

Architecture: 3-Tier

Brisbane Branch:

Type: LAN/WAN

Topology: Dual-Star high availability

Architecture: 2-Tier

Network Nodes

Sydney		Brisbane
2 (HA)	Routers	2
5	Switches	5
2 (HA)	Switches L3	2 (HA)
1x1x0	Servers, Printers, Modems	0x1x2
1	End Devices	19

Content

- Legal & security: Policies and Procedures
- WAN Configuration and Troubleshooting & Testing
- Summary Technologies & Protocols

Legal & security: Policies and Procedures

Legal & security

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

Legal & security

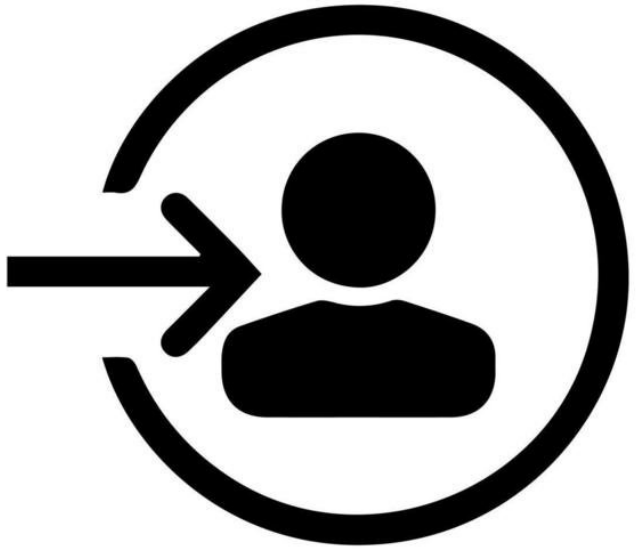
Service Password Encryption

Policy to prevent access to plain-text passwords in network devices.

ISO/IEC 27001

Mandatory Login Password

Policy on all network devices that requires a login password for any access to routers or switches.

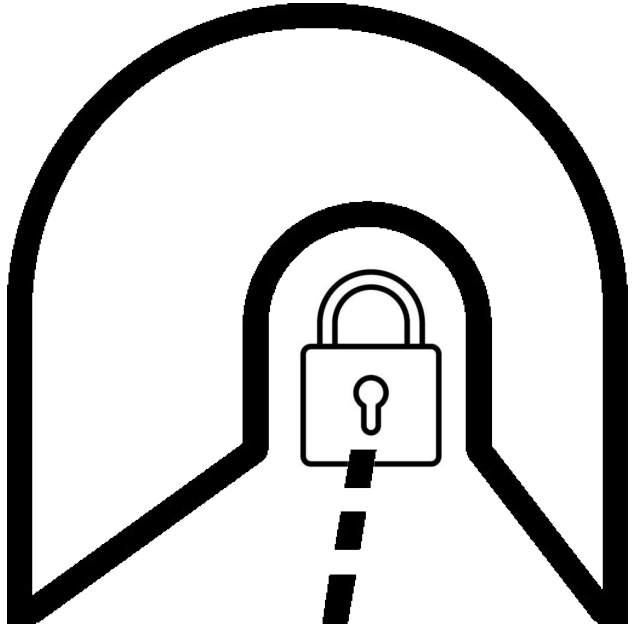


NIST SP 800-53 (IA-2)

Legal & security

VPN Site-to-Site

Policy implements IPSec to protect data in transit between different company branches over internet.



NIST SP 800-77

Legal & security

Access Control Lists (ACLs)

Policy to filter traffic and control access between subnets, enhance internal network security.

ISO/IEC 27002 (s13)

Legal & security

Secure Remote Access to infrastructure

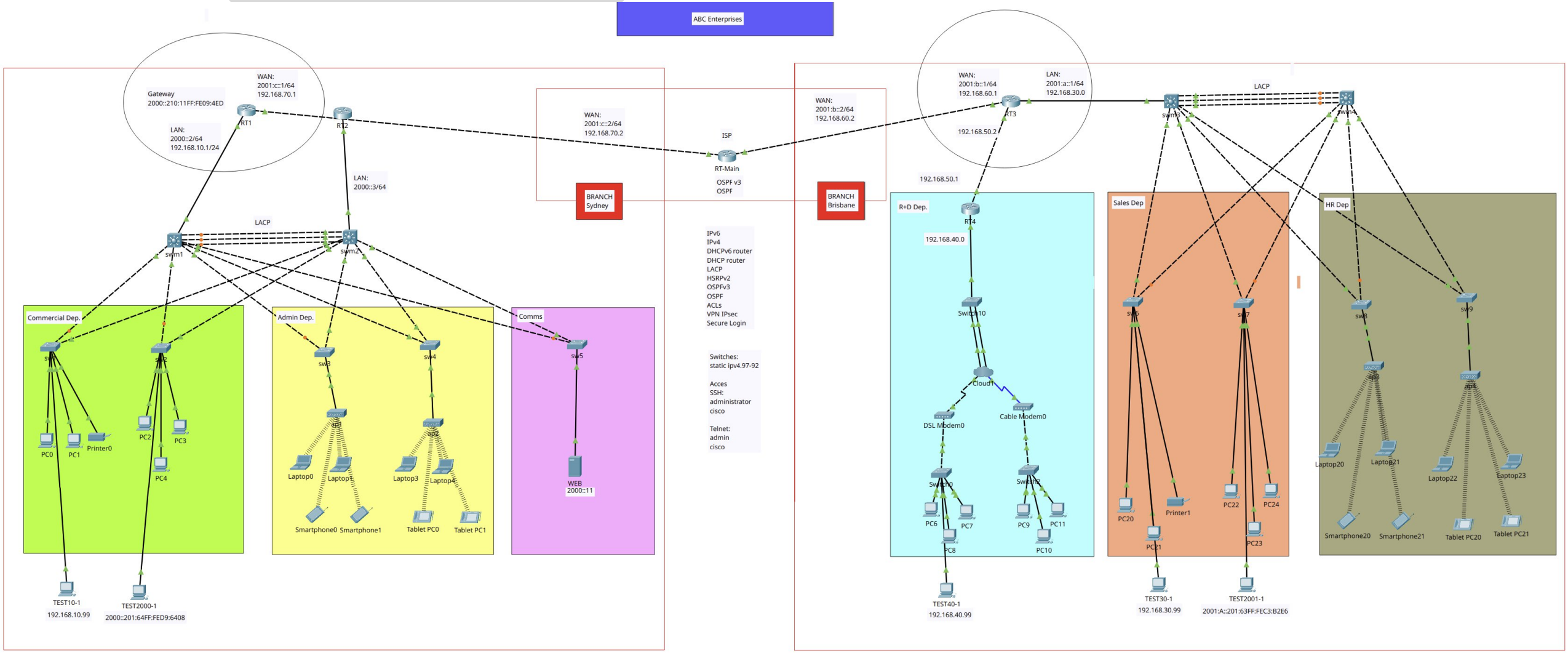
Policy to protect remote access by Telnet and SSH to network devices using password-protected and encrypted.

NIST SP 800-5

WAN Configuration

Installation Plan

Network


ABC Enterprises
Gateway
2000::210:11FF:FE09:4ED
WAN:
2001:c::1/64
192.168.70.1
LAN:
2000::2/64
192.168.10.1/24
RT1
RT2
LAN:
2000::3/64
LACP
swm1
swm2
WAN:
2001:c::2/64
192.168.70.2
ISP
RT-Main
OSPF v3
OSPF
BRANCH
Sydney
BRANCH
Brisbane
WAN:
2001:b::2/64
192.168.60.2
WAN:
2001:b::1/64
192.168.60.1
LAN:
2001:a::1/64
192.168.30.0
RT3
192.168.50.2
192.168.50.1
swm3
swm4
LACP
IPv6
IPv4
DHCPv6 router
DHCP router
LACP
HSRPv2
OSPFv3
OSPF
ACLs
VPN IPsec
Secure Login
Switches:
static ipv4.97-92
Acces
SSH:
administrator
cisco
Telnet:
admin
cisco
Commercial Dep.
sw1
sw2
PC0
PC1
Printer0
PC2
PC3
PC4
Admin Dep.
sw3
sw4
ap1
ap2
Laptop0
Laptop1
Laptop3
Laptop4
Smartphone0
Smartphone1
Tablet PC0
Tablet PC1
Comms
sw5
WEB
2000::11
TEST10-1
192.168.10.99
TEST2000-1
2000::201:64FF:FED9:6408
R+D Dep.
RT4
192.168.40.0
Switch10
Cloud1
DSL Modem0
Cable Modem0
Switch0
Switch2
PC6
PC7
PC8
PC9
PC11
PC10
TEST40-1
192.168.40.99
Sales Dep
sw6
sw7
PC20
Printer1
PC21
PC22
PC24
PC23
TEST30-1
192.168.30.99
TEST2001-1
2001:A::201:63FF:FEC3:B2E6
HR Dep
sw8
sw9
ap3
ap4
Laptop20
Laptop21
Laptop22
Laptop23
Smartphone20
Smartphone21
Tablet PC20
Tablet PC21

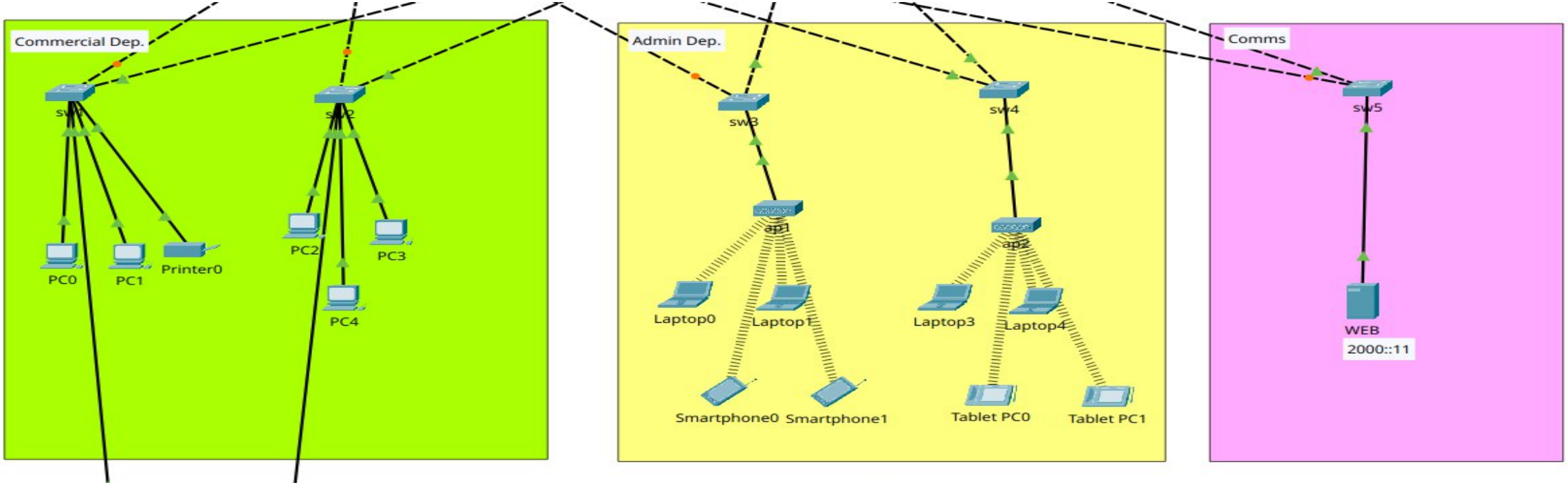
WAN Configuration

- Secure Access by SSH & Telnet
- Additional Protocols: DHCP
- Additional Protocols: LACP
- Additional Protocols: HSRP
- Additional Protocols: OSPF
- Additional Protocols: OSPF
- WAN protocols: ACL
- WAN Protocols: VPN
- WAN Protocols: PPP
- Dynamic NAT
- Firewall Single-port
- Logging Network

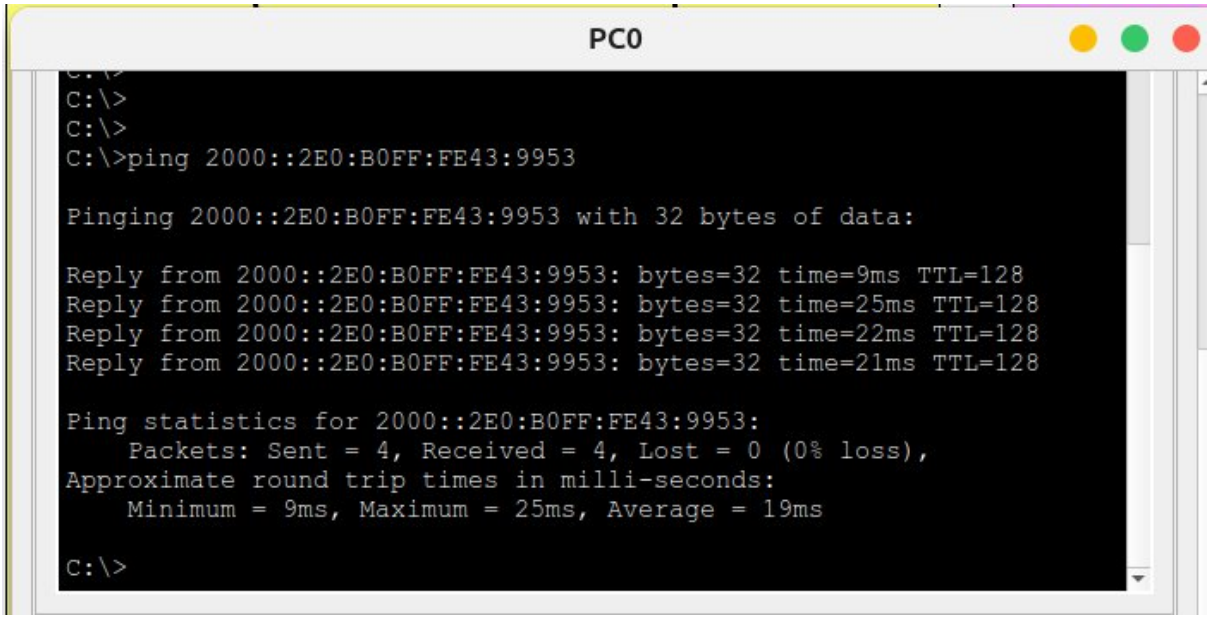
Troubleshooting & Testing

Local

Sydney Branch

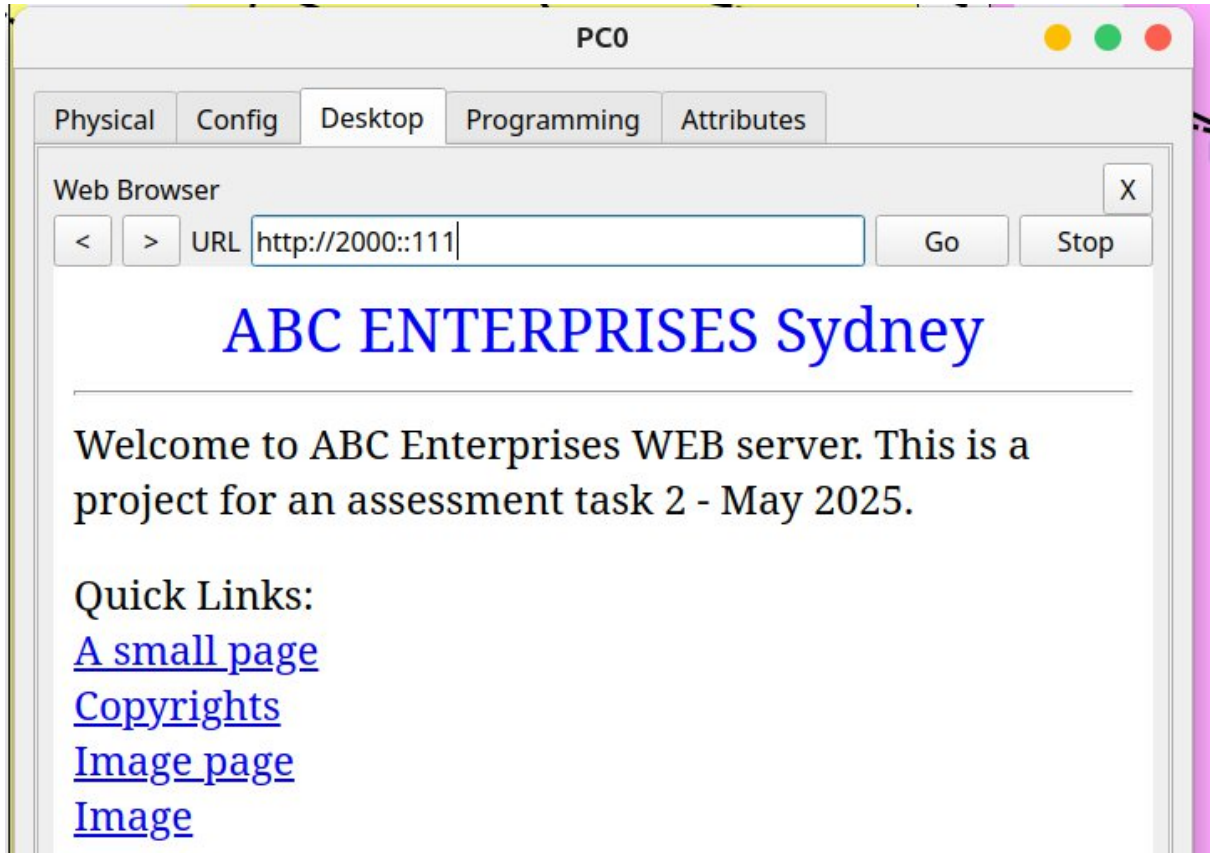


Sydney Branch - Local



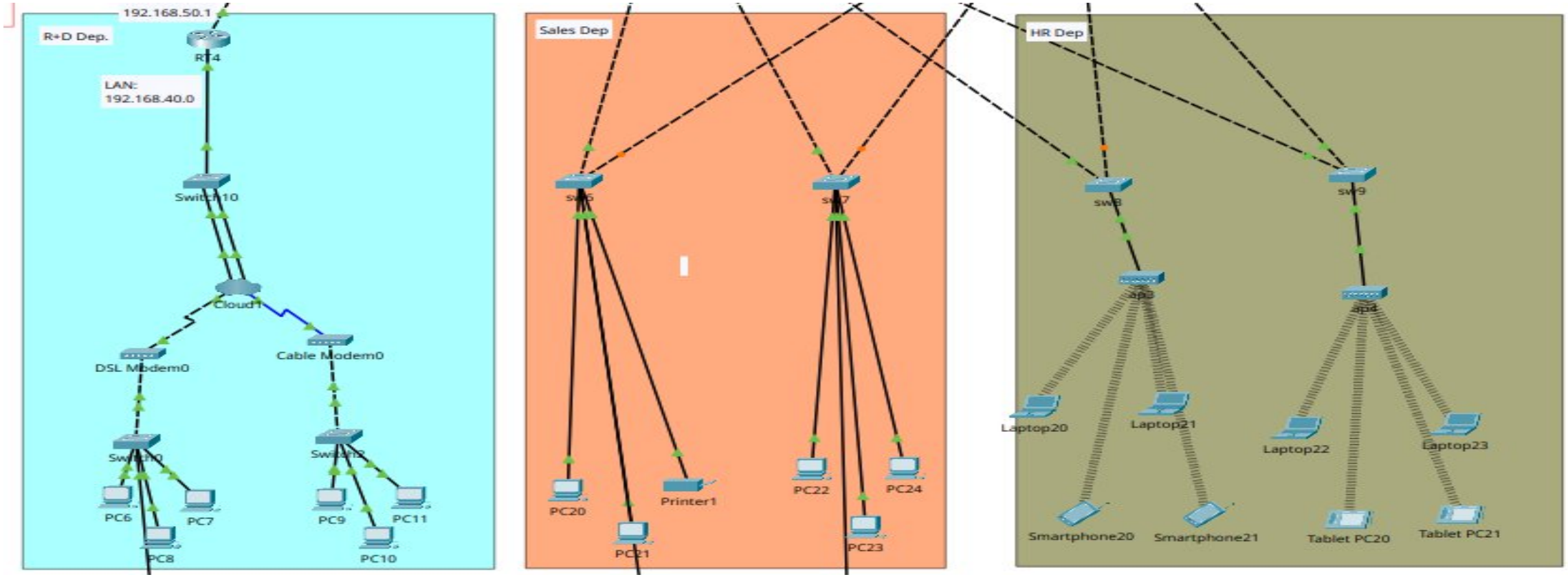
Commercial and Admin over IPv6PC0 LAPTOP0

Sydney Branch - Local

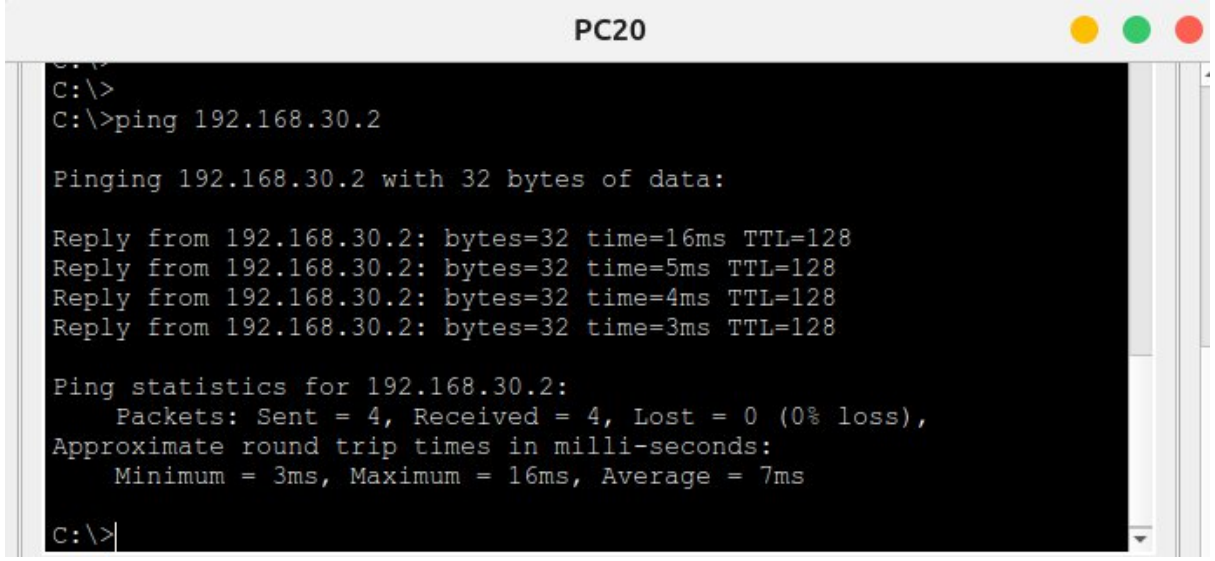


Commercial and Comms over IPv6
WEB PC0

Brisbane Branch

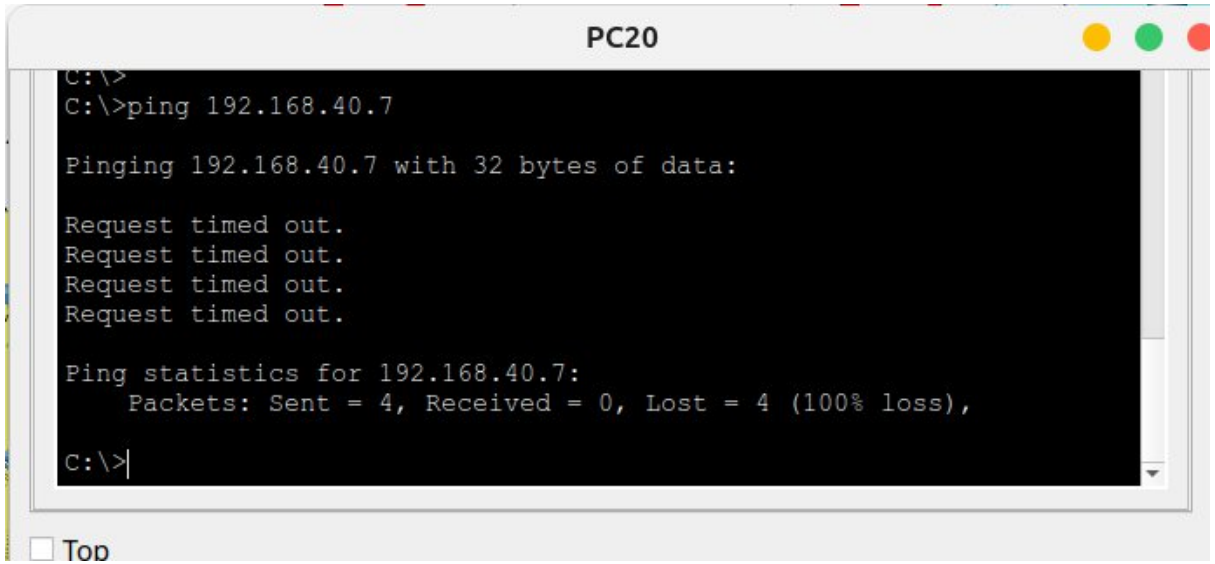


Brisbane Branch - Local



Sales and HR over IPv4
PC20 LAPTOP20

Brisbane Branch - Local



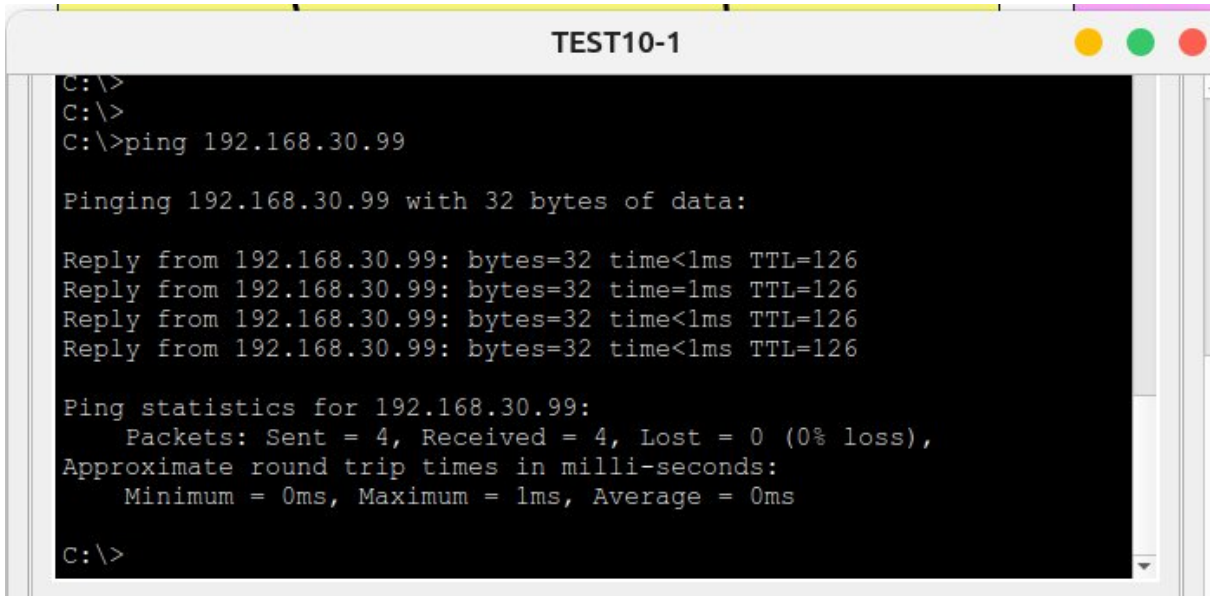
Sales and R+D
HR and R+D over IPv4

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

Troubleshooting & Testing

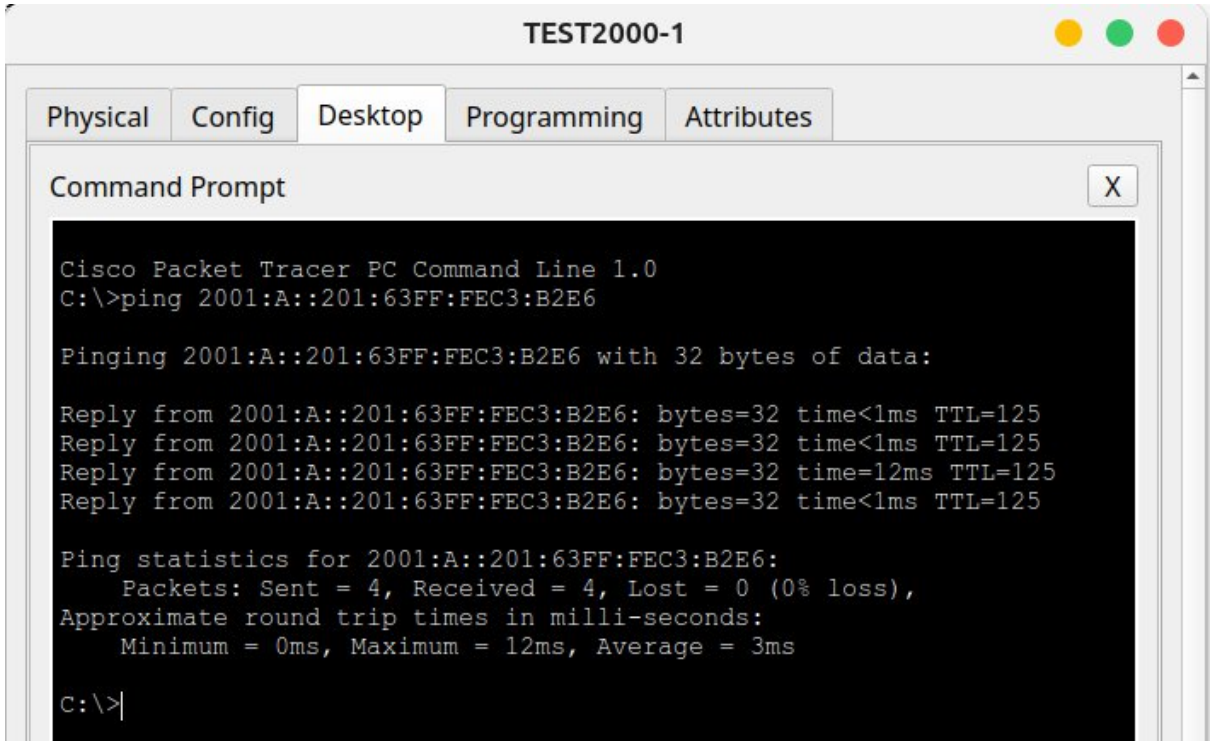
WAN

WAN



Sydney Branch and Brisbane Branch over IPv4

WAN

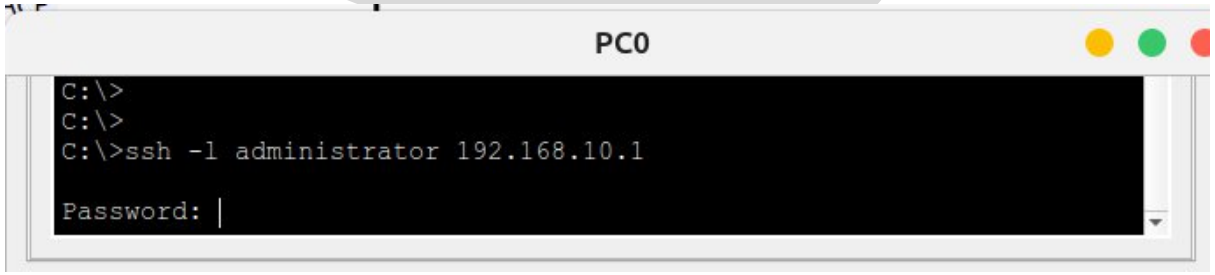


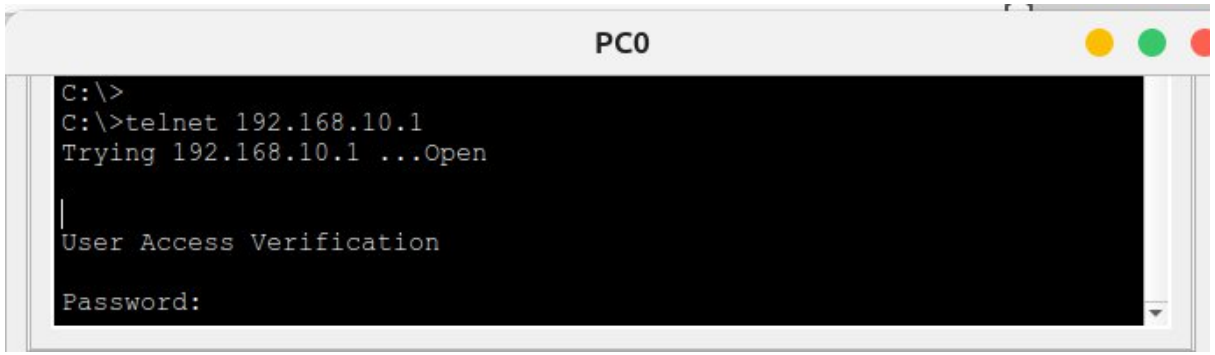
Brisbane Branch and Sydney Branch over IPv6

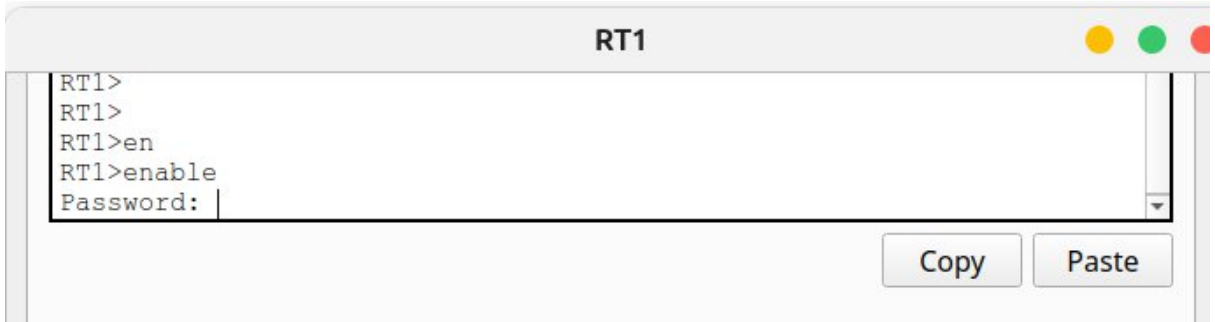
Secure Access SSH & Telnet

WAN

Secure Access



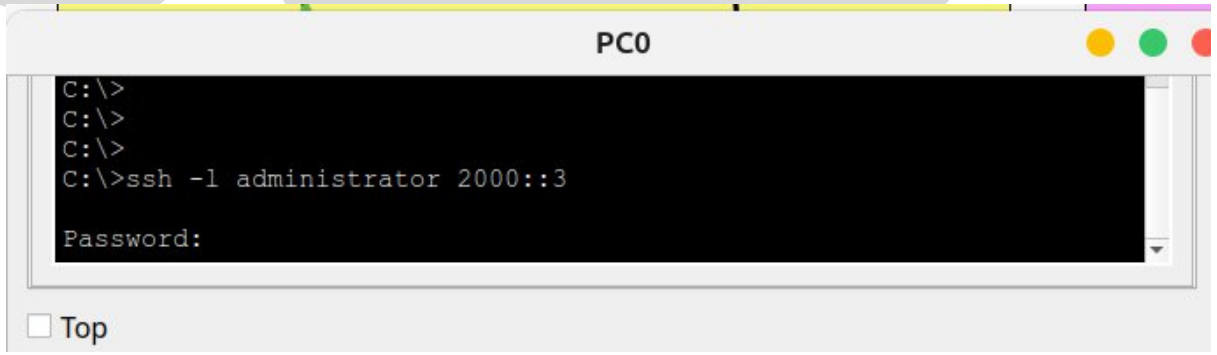


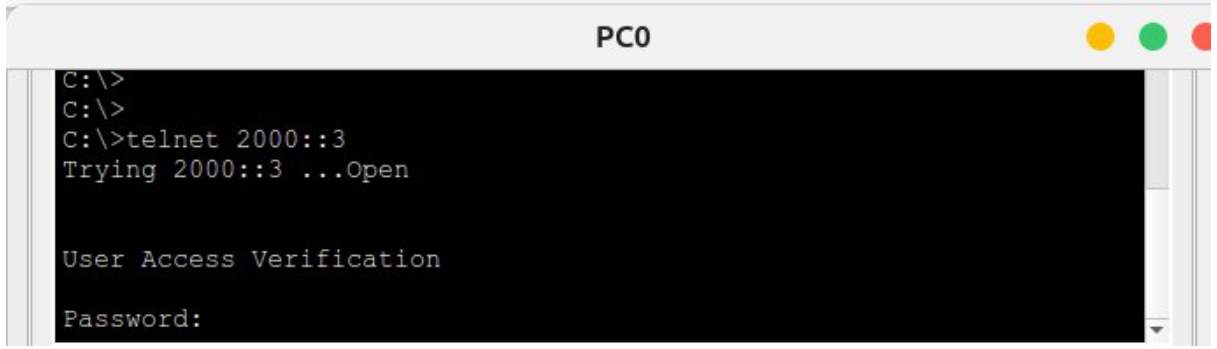


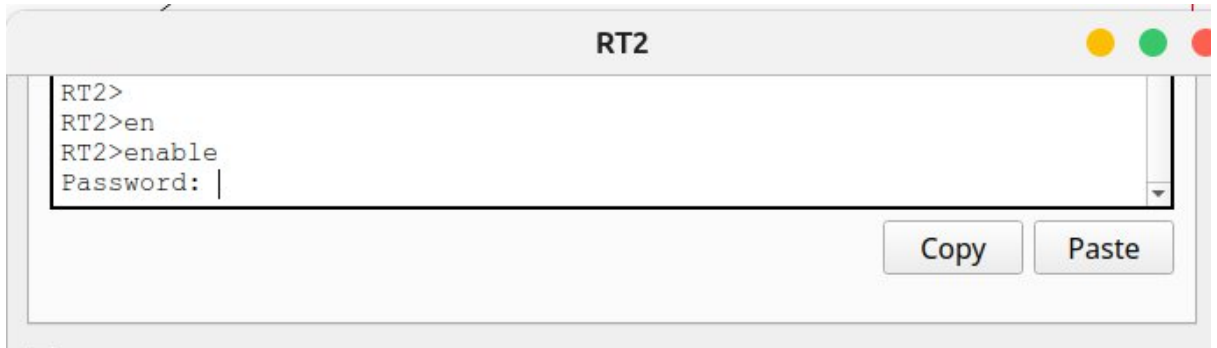
RT1

192.168.10.1

Secure Access



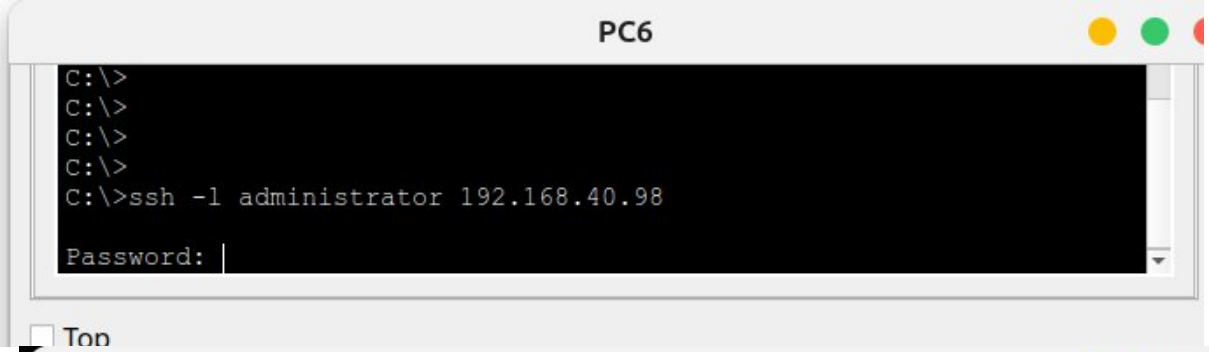


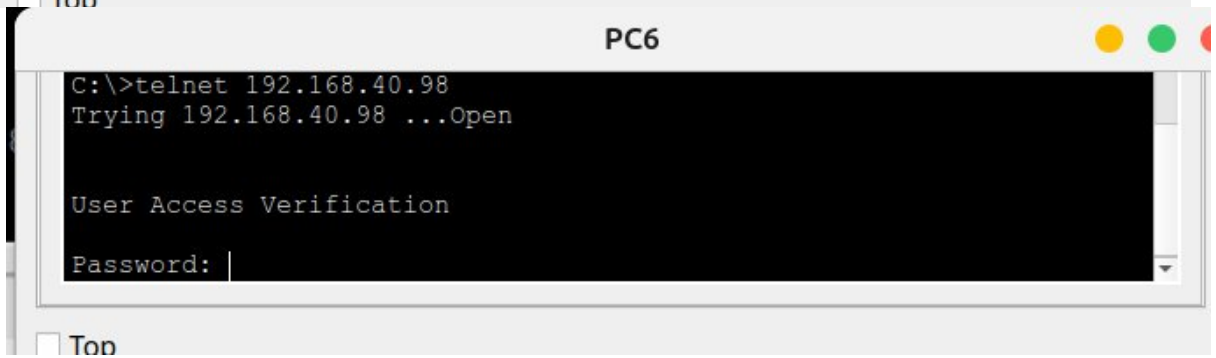


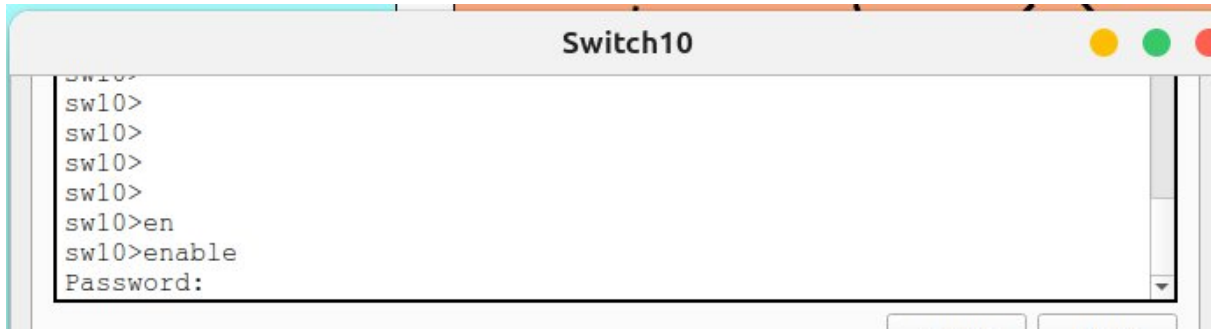
RT2

2000::3

Secure Access







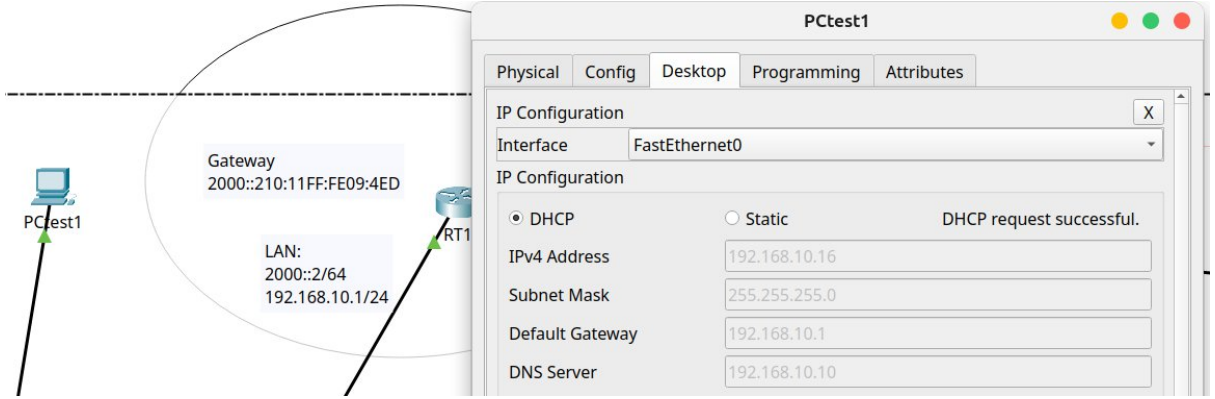
sw10

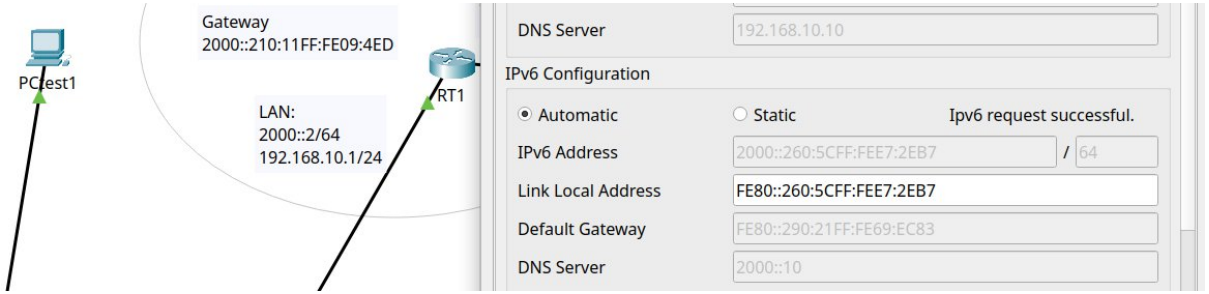
VLAN1:192.168.40.98

DHCP

WAN

Sydney Branch

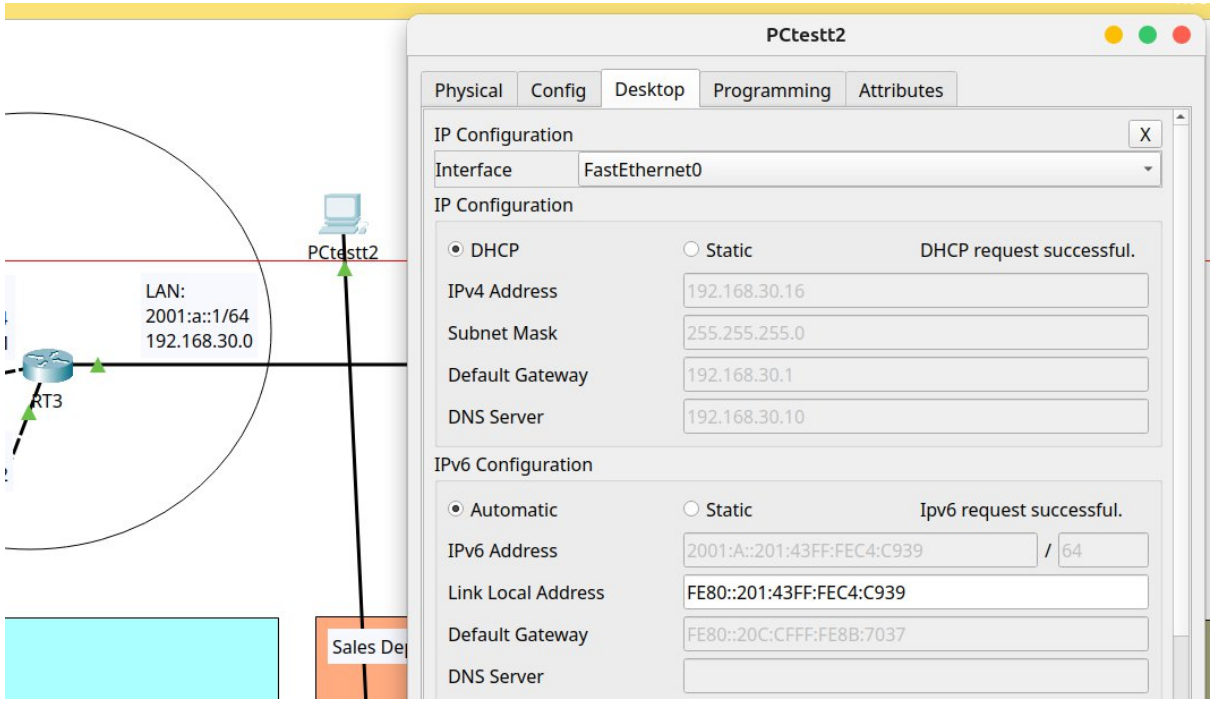




RT1

New PC configured to DHCP and IPv6 Auto

Brisbane Branch



RT3

New PC configured to DHCP and IPv6 Auto

Testing LACP

WAN – IPv6

Summary port-channel

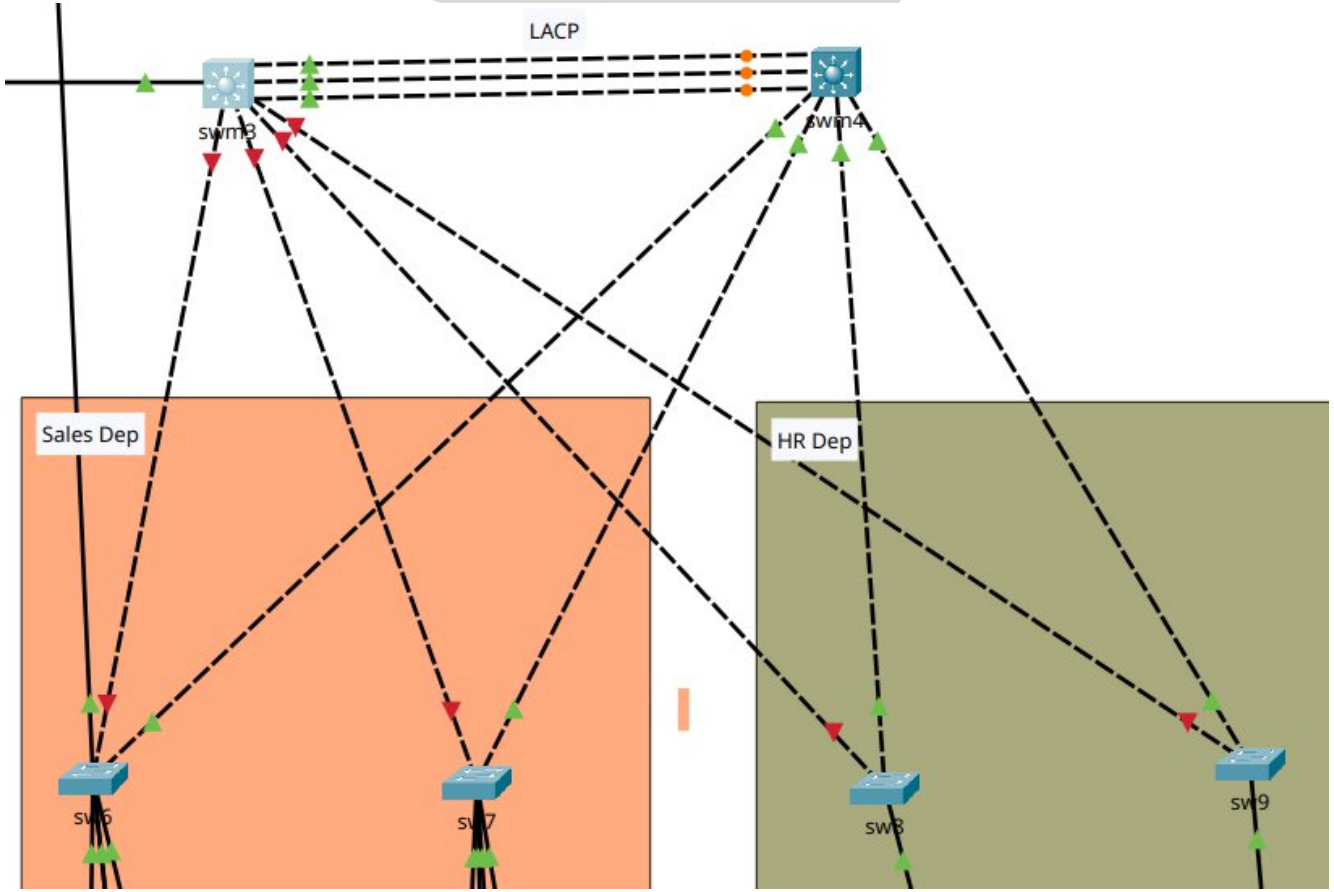
swm1

```
swm1#show et
swm1#show etherchannel su
swm1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)           LACP   Gig1/0/22(P) Gig1/0/23(P) Gig1/0/24(P)
```

Sydney

Summary config

LACP - Brisbane Branch



- Turned Down swm3 interfaces

Brisbane Branch

Laptop20

```
Pinging 2001:a::99 with 32 bytes of data:

Reply from 2001:A::99: bytes=32 time=34ms TTL=128
Reply from 2001:A::99: bytes=32 time=20ms TTL=128
Reply from 2001:A::99: bytes=32 time=11ms TTL=128
Reply from 2001:A::99: bytes=32 time=16ms TTL=128

Ping statistics for 2001:A::99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Smartphone20

```
Pinging 192.168.10.99 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.99: bytes=32 time=20ms TTL=126
Reply from 192.168.10.99: bytes=32 time=34ms TTL=126
Reply from 192.168.10.99: bytes=32 time=22ms TTL=126

Ping statistics for 192.168.10.99:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

- Connections are still working...

Testing HSRP

Sydney – IPv6

HSRP

Primary (priority 120) and secondary router (priority 100).

RT1

```
RT1#
RT1#
RT1#
RT1#
RT1#
RT1# show standby
GigabitEthernet0/0 - Group 1 (version 2)
  State is Active
    7 state changes, last state change 00:00:18
  Virtual IP address is FE80::5:73FF:FEA0:1
  Active virtual MAC address is 0005.73A0.0001
    Local virtual MAC address is 0005.73A0.0001 (v2 IPv6
default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.755 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 120 (configured 120)
  Group name is hsrp-Gig0/0-1 (default)
RT1#
```

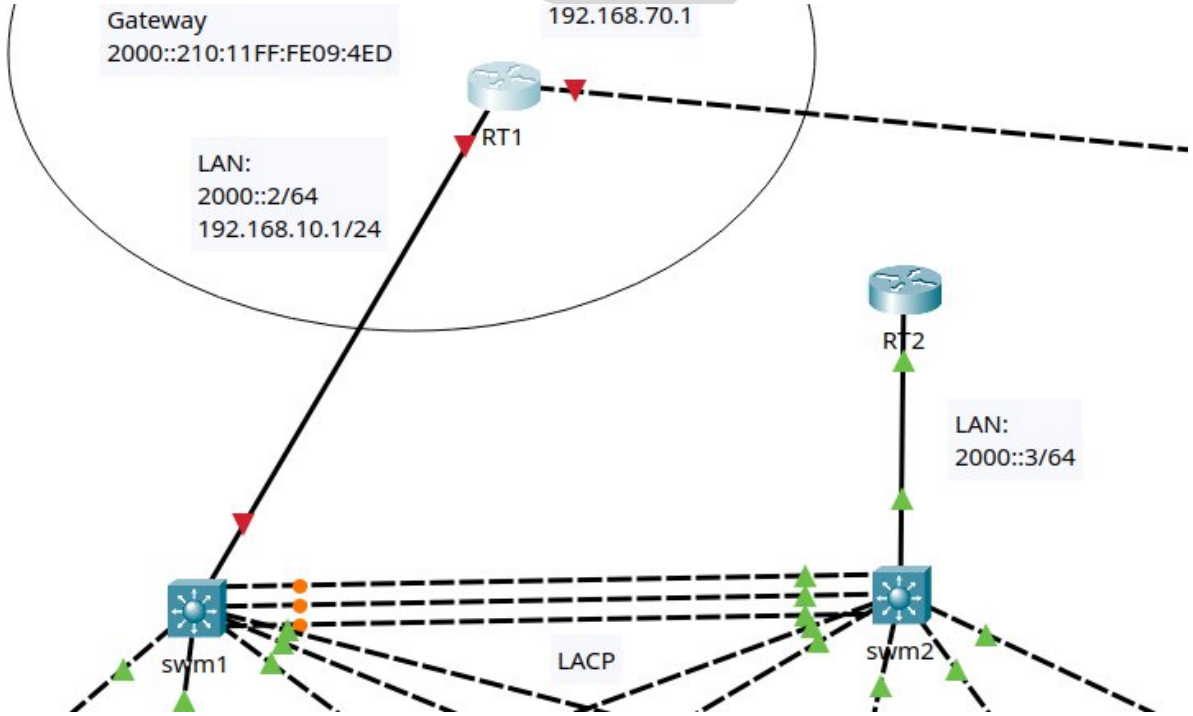
Copy Paste

RT2

```
RT2#
RT2#
RT2#
RT2#
RT2#
RT2#show standby
GigabitEthernet0/0 - Group 1 (version 2)
  State is Active
    7 state changes, last state change 00:00:18
  Virtual IP address is FE80::5:73FF:FEA0:1
  Active virtual MAC address is 0005.73A0.0001
    Local virtual MAC address is 0005.73A0.0001 (v2 IPv6
default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.539 secs
  Preemption disabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  Group name is hsrp-Gig0/0-1 (default)
RT2#
```

Copy Paste

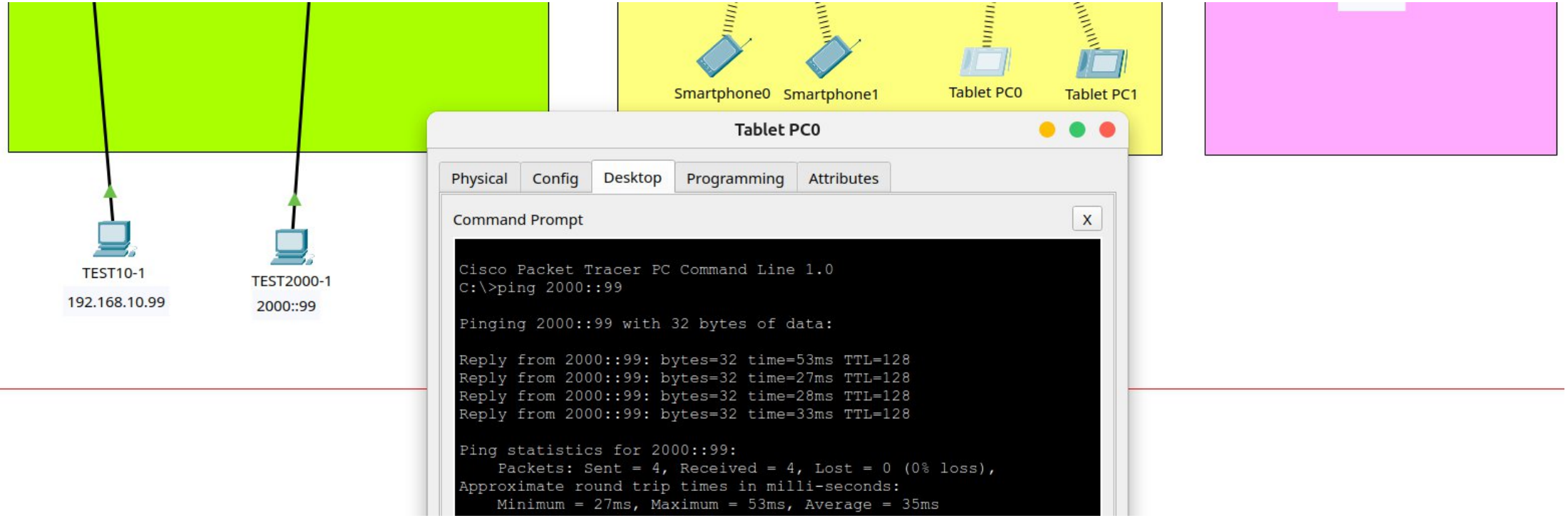
HSRP



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

HSRP

RT2 keeps LAN working...



Testing OSPF

WAN

HSRP

Routes between devices are proved by OSPF

RT1

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
RT1#
RT1#
RT1#
RT1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
O    192.168.30.0/24 [110/3] via 192.168.70.2, 00:21:00, GigabitEthernet0/1
O    192.168.40.0/24 [110/4] via 192.168.70.2, 00:21:00, GigabitEthernet0/1
O    192.168.50.0/24 [110/3] via 192.168.70.2, 00:21:00, GigabitEthernet0/1
O    192.168.60.0/24 [110/2] via 192.168.70.2, 00:21:00, GigabitEthernet0/1
     192.168.70.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.70.0/24 is directly connected, GigabitEthernet0/1
L       192.168.70.1/32 is directly connected, GigabitEthernet0/1
```

RT3

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
RT3#
RT3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    192.168.10.0/24 [110/3] via 192.168.60.2, 00:21:20, GigabitEthernet0/1
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, GigabitEthernet0/2
L       192.168.30.1/32 is directly connected, GigabitEthernet0/2
O    192.168.40.0/24 [110/2] via 192.168.50.1, 01:20:37, GigabitEthernet0/0
     192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/24 is directly connected, GigabitEthernet0/0
L       192.168.50.2/32 is directly connected, GigabitEthernet0/0
     192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.60.0/24 is directly connected, GigabitEthernet0/1
L       192.168.60.1/32 is directly connected, GigabitEthernet0/1
O    192.168.70.0/24 [110/2] via 192.168.60.2, 00:22:05, GigabitEthernet0/1
```

HSRP

Routes between devices are proved by OSPFv3

RT1

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
RT1#
RT1#show ipv
RT1#show ipv6 ro
RT1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2000::/64 [0/0]
     via GigabitEthernet0/0, directly connected
L   2000::2/128 [0/0]
     via GigabitEthernet0/0, receive
O   2001:A::/64 [110/3]
     via FE80::201:42FF:FEE2:2C3, GigabitEthernet0/1
O   2001:B::/64 [110/3]
     via FE80::201:42FF:FEE2:2C3, GigabitEthernet0/1
C   2001:C::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:C::1/128 [0/0]
     via GigabitEthernet0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

RT3

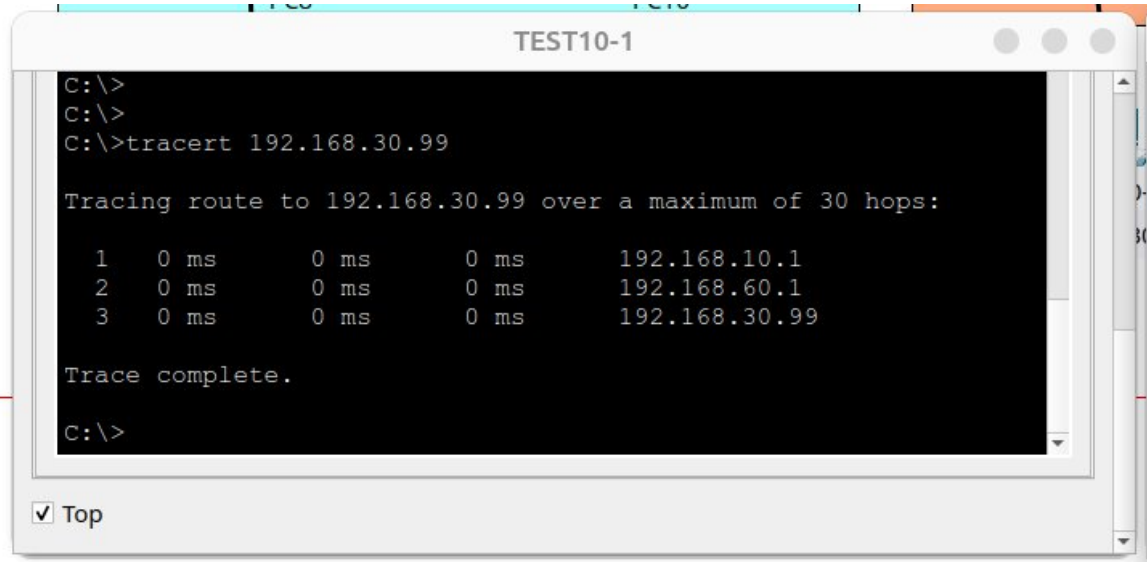
Physical | Config | CLI | Attributes

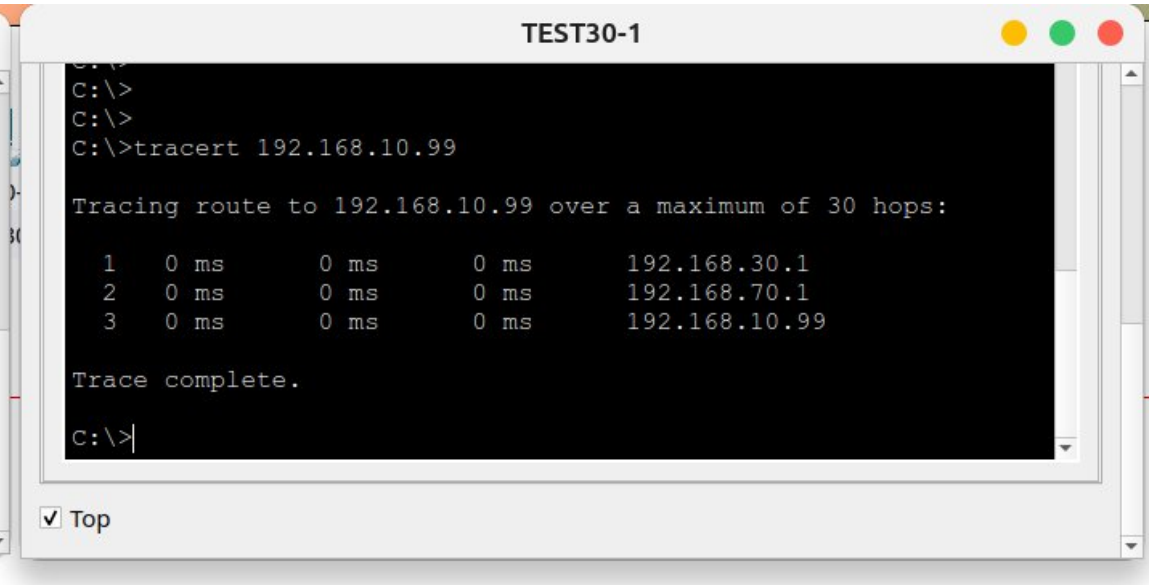
IOS Command Line Interface

```
RT3#show ipv6 ro
RT3#show ipv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
O   2000::/64 [110/3]
     via FE80::20D:BDFF:FE6A:2CBB, GigabitEthernet0/1
C   2001:A::/64 [0/0]
     via GigabitEthernet0/2, directly connected
L   2001:A::1/128 [0/0]
     via GigabitEthernet0/2, receive
C   2001:B::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:B::1/128 [0/0]
     via GigabitEthernet0/1, receive
O   2001:C::/64 [110/2]
     via FE80::20D:BDFF:FE6A:2CBB, GigabitEthernet0/1
O   2010::/64 [110/2]
     via FE80::20D:BDFF:FE6A:2CBB, GigabitEthernet0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

HSRP

Bidirectional trace route between Sydney Branch and Brisbane Branch over IPv4





HSRP

Bidirectional trace route between Sydney Branch and Brisbane Branch over IPv6

TEST2000-99_

```
C:\>
C:\>tracert 2001:a::99

Tracing route to 2001:a::99 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      2000::2
  2   0 ms      0 ms      0 ms      2001:C::2
  3   0 ms      0 ms      0 ms      2001:B::1
  4   0 ms      0 ms      0 ms      2001:A::99

Trace complete.
```

TEST2001A-1

```
C:\>tracert 2000::99

Tracing route to 2000::99 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      2001:A::1
  2   0 ms      0 ms      0 ms      2001:B::2
  3   0 ms      0 ms      0 ms      2001:C::1
  4   0 ms      0 ms      0 ms      2000::99

Trace complete.
```

Testing ACL

WAN – IPv4

ACL

Example ACL on R1 (Sydney Branch)

RT1

```
RT1#
RT1#
RT1#show access-lists
Extended IP access list 110
    10 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
    20 permit ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
(1 match(es))
    30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
    40 permit ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
```

ACL

Deny rule for testing traffic from 192.168.10.99 (Brisbane)

```
RT1#show access-lists
Extended IP access list 110
    10 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
    20 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
```

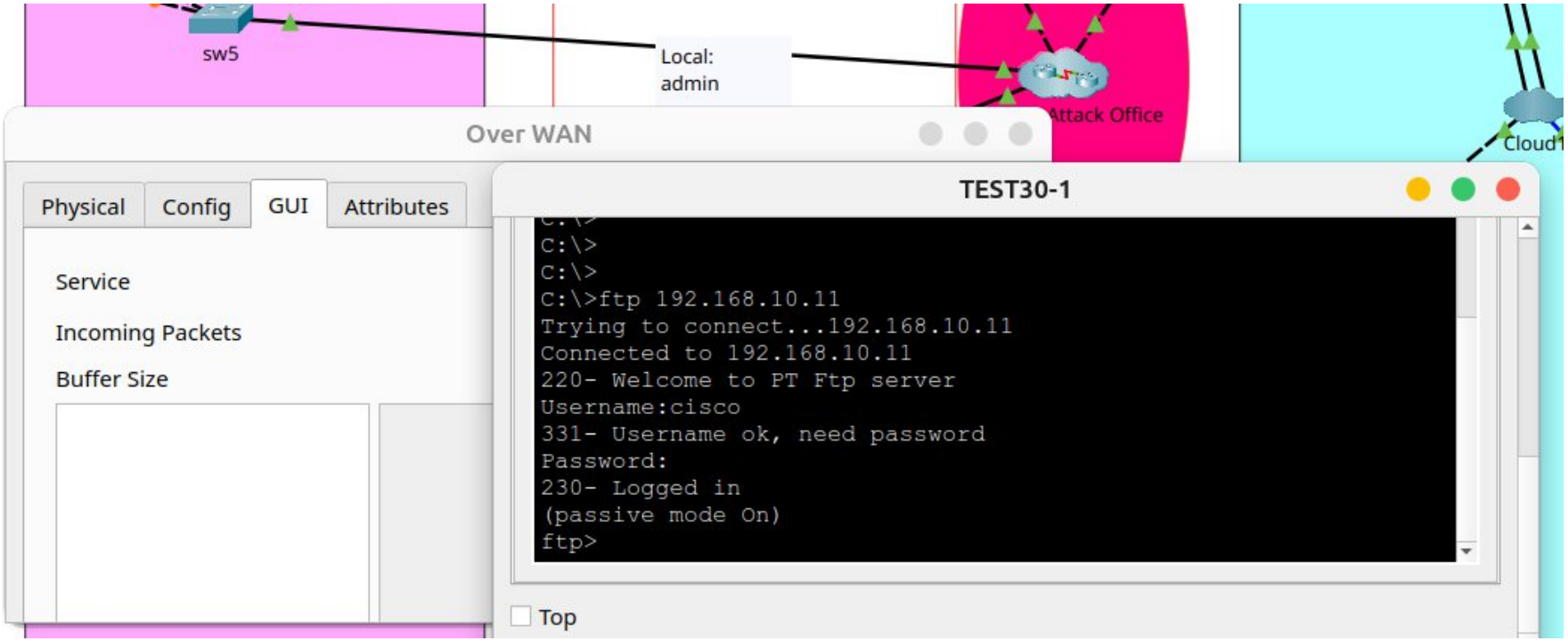
```
Pinging 192.168.10.99 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.99:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Testing VPN Site-To-Site

WAN – IPv4

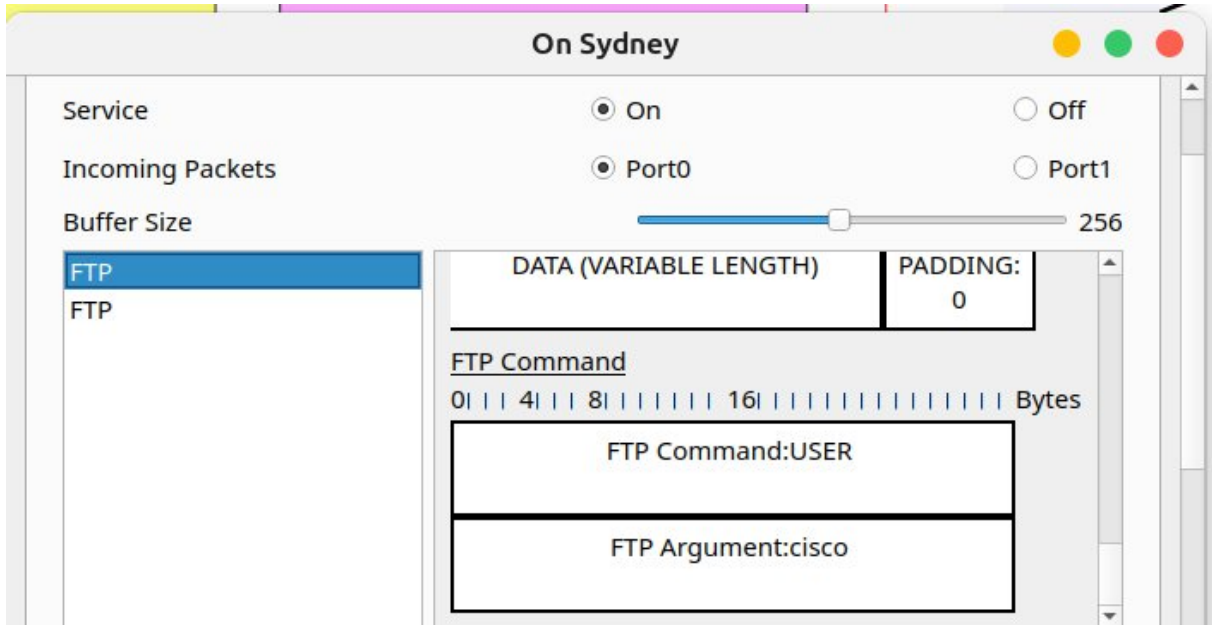
VPN Site-To-Site

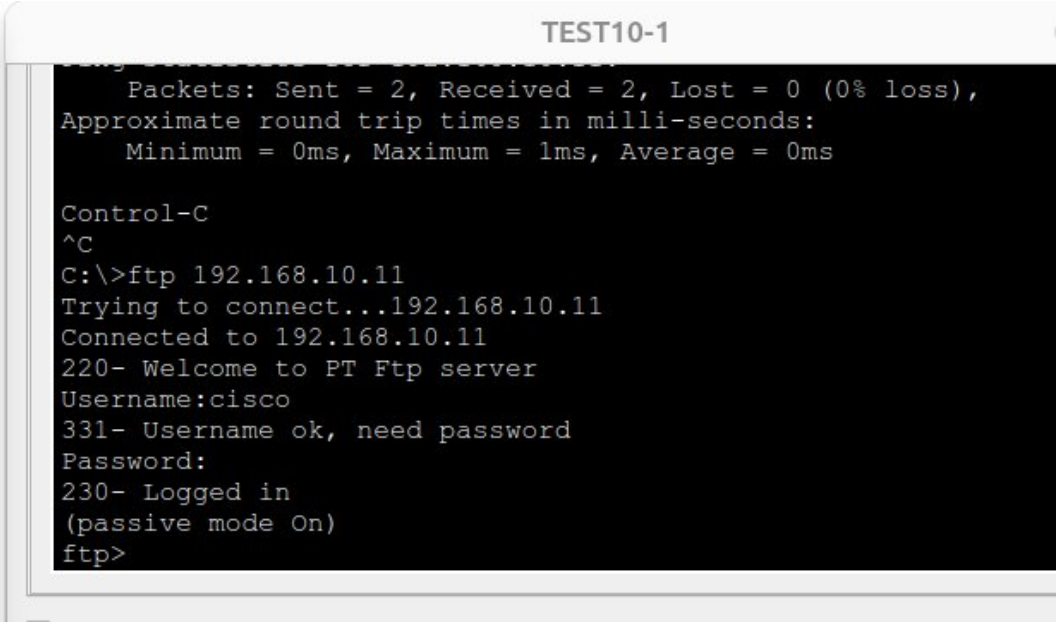
Internet connection are intercepted by a criminal sniffer.
FTP Messages cannot be captured.



VPN Site-To-Site

Local connection are susceptible to attacks.
FTP Messages can be captured.

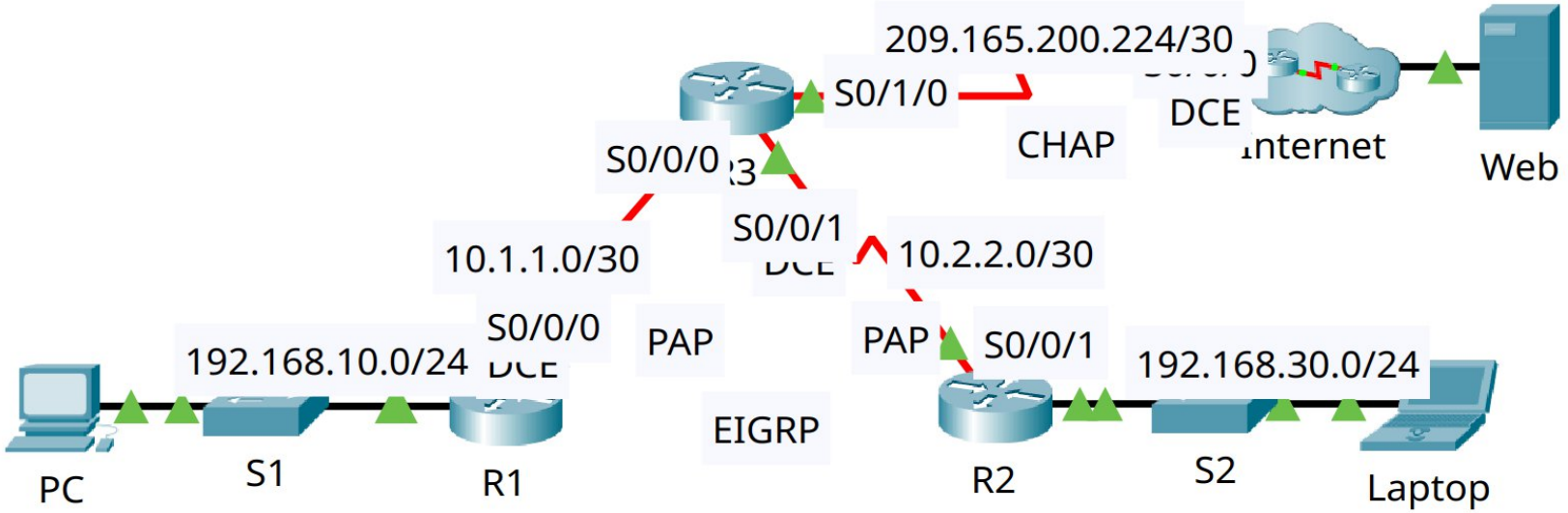


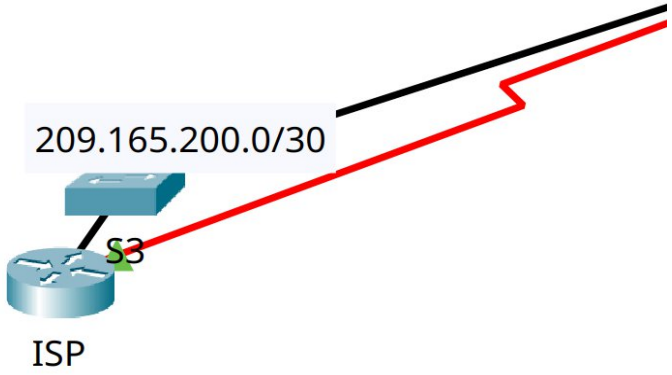


Testing Encapsulation PPP

IPv4

Encapsulation PPP





Implemented CHAP as an automatic authentication method.

Encapsulation PPP

Connection from Local network to WEB server are working under encapsulation method. CHAP implemented.

PC

Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.2

Pinging 209.165.200.2 with 32 bytes of data:

Request timed out.
Reply from 209.165.200.2: bytes=32 time=55ms TTL=125
Reply from 209.165.200.2: bytes=32 time=70ms TTL=125
Reply from 209.165.200.2: bytes=32 time=48ms TTL=125

Ping statistics for 209.165.200.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 48ms, Maximum = 70ms, Average = 57ms

C:\>
```

Laptop

Physical | Config | Desktop | Programming | Attributes

Command Prompt

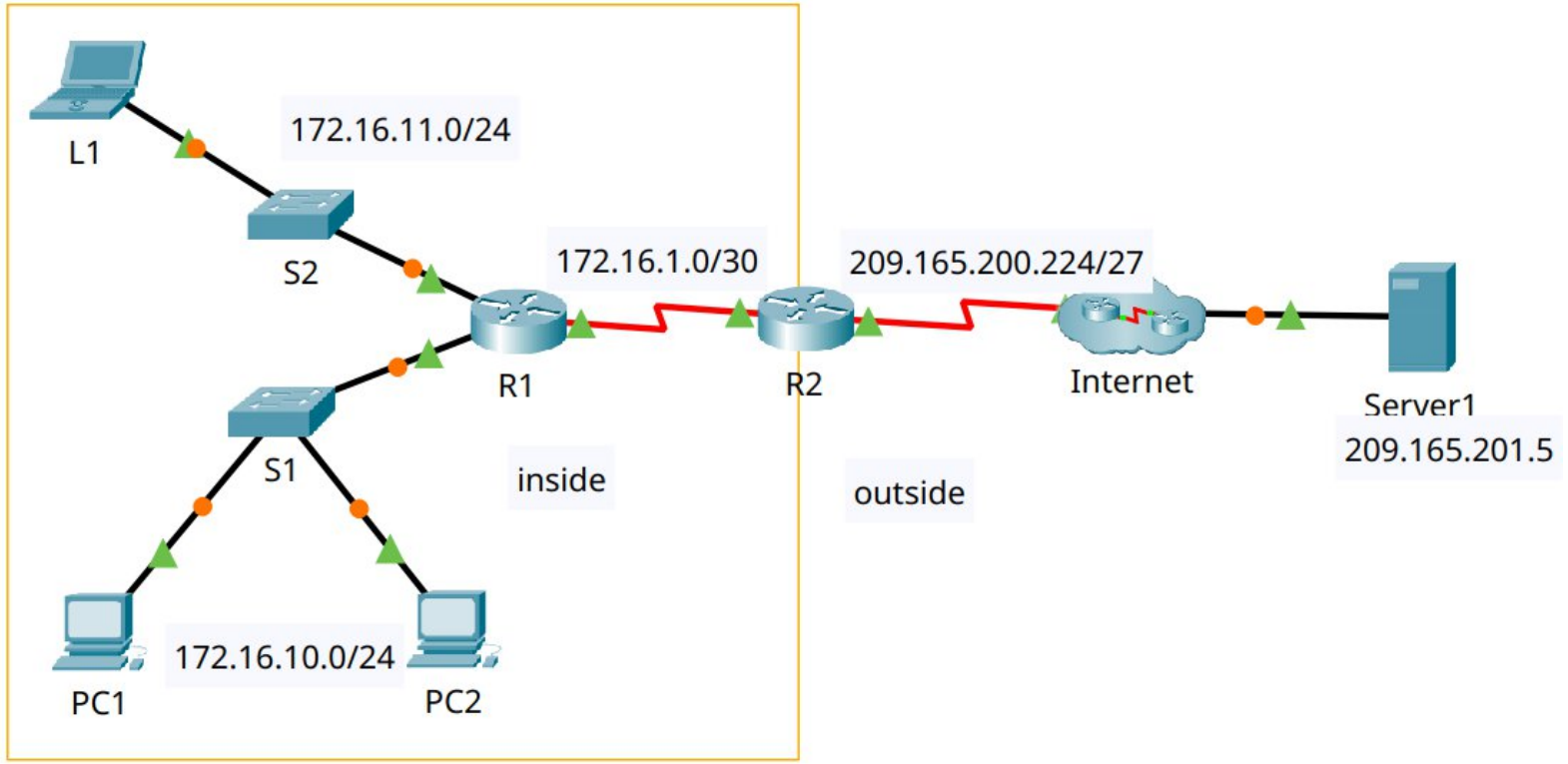
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.2

Pinging 209.165.200.2 with 32 bytes of data:

Reply from 209.165.200.2: bytes=32 time=59ms TTL=125
Reply from 209.165.200.2: bytes=32 time=82ms TTL=125
Reply from 209.165.200.2: bytes=32 time=62ms TTL=125
Reply from 209.165.200.2: bytes=32 time=58ms TTL=125

Ping statistics for 209.165.200.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 58ms, Maximum = 82ms, Average = 65ms

C:\>
```

Dynamic NAT

IPv4

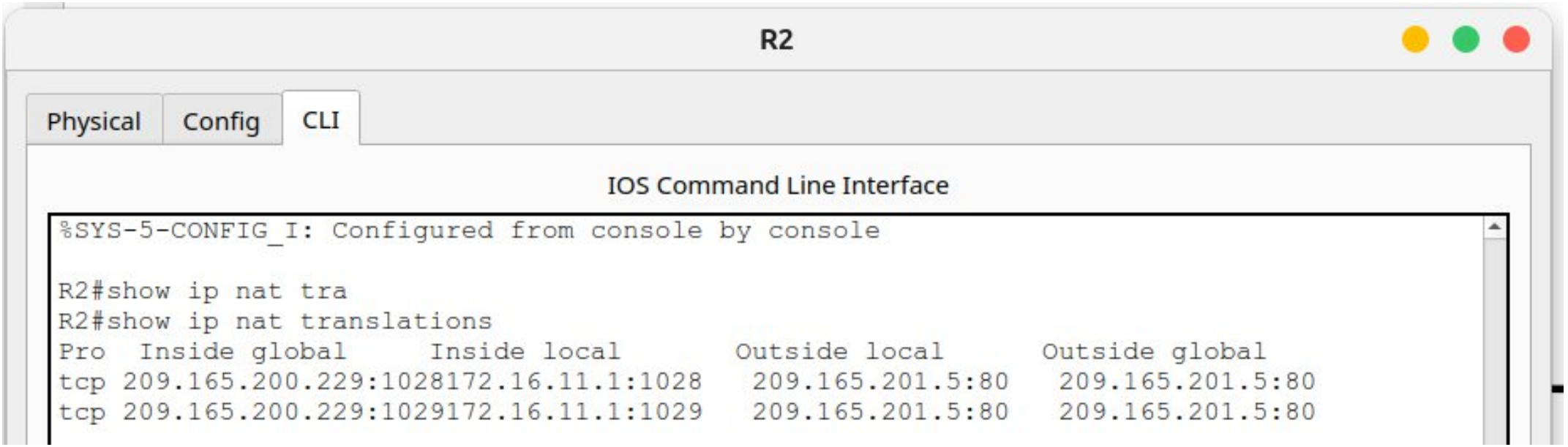
Dynamic NAT

WAN Network



Dynamic NAT

R2 NAT Translations table on



Dynamic NAT

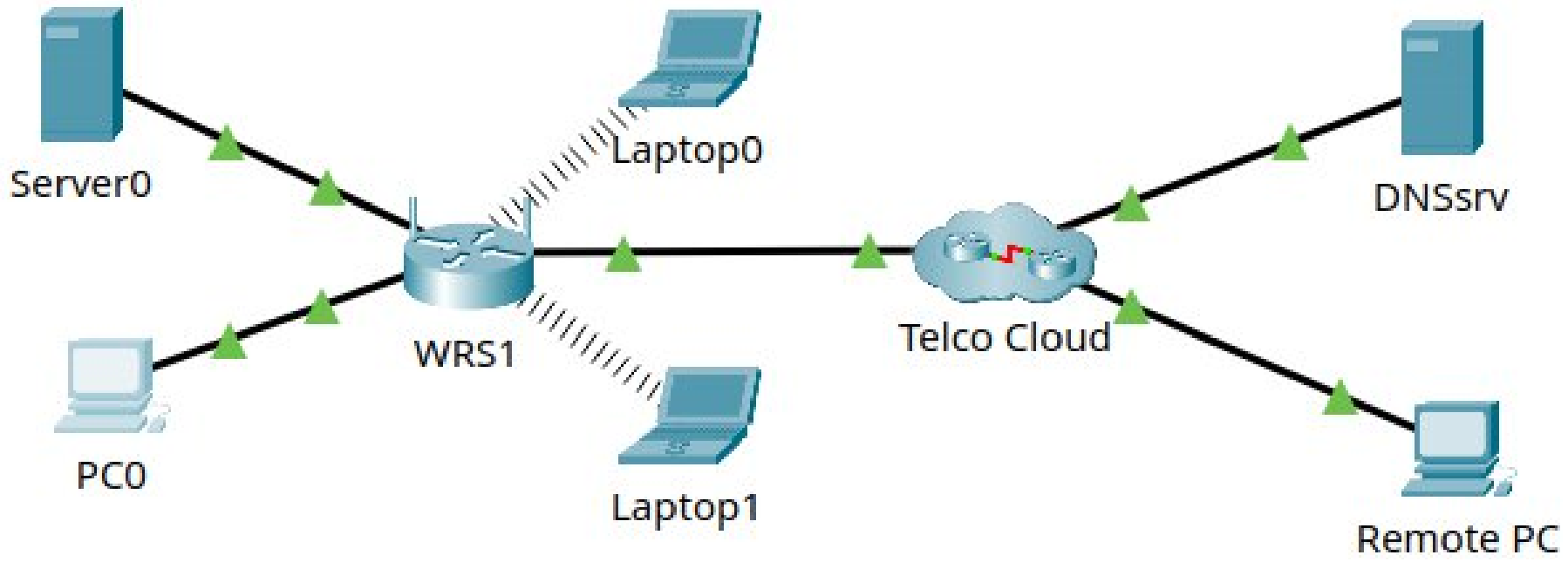
Testing WEB connection

Testing Firewall and Single-port

IPv4

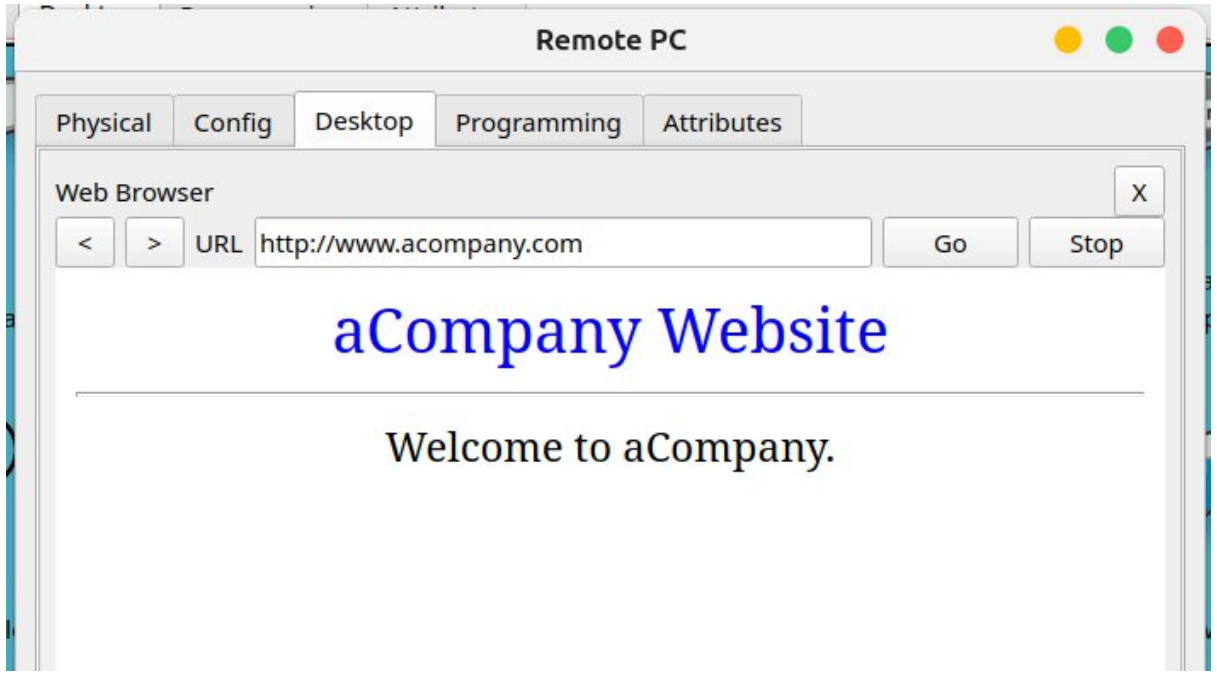
Firewall Single-port

WAN network



Firewall Single-port

Single-port enabled and DMZ disabled



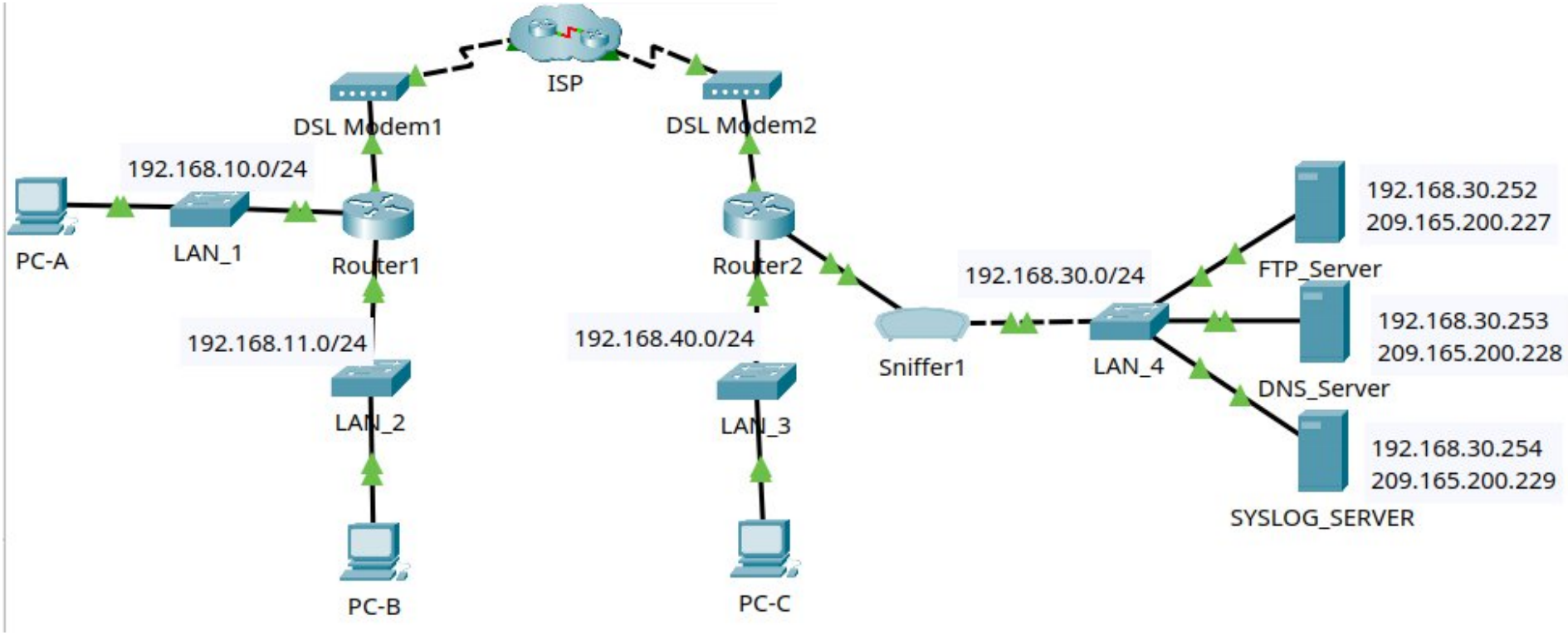
Connection from Remote PC to WEB Server

Logging Network

IPv4

Logging

WAN Network



Logging

Echo replies from R2 to PC-C its destination is LAN interface of R2 (because is its local network)

Syslog

Service ◉ On ○ Off

	Time	HostName	Message
1	02.13.2020 ...	192.168.30.1	.1, dst 192.168.40.2
2	02.13.2020 ...	192.168.30.1	...
3	02.13.2020 ...	192.168.30.1	...
4	02.13.2020 ...	192.168.30.1	...

Summary Technologies & Protocols

Summary Technologies

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.

Summary Technologies

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.

Summary Technologies

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.

Summary Technologies

PPP Authentication (Point-to-Point Protocol Authentication):
Responsible for establishing point-to-point connections and provides encapsulation to facilitate the connection. Also supports authentication mechanisms (CHAP) between two network devices to add an additional layer of security.

Summary Technologies

Dynamic NAT (Dynamic Network Address Translation): Map a public network to multiple private networks on a WAN to communicate with external IPs..

Bibliography

- Network System: Gurutech Networking Training - Secure Network Training
- DHCPv6 Router: Gurutech Networking Training - DHCPv6
- DHCPv6 stateless-stateful: ShefferKimanzi - DCHP v6 configuration
- LACP: ITExamAnswers.net - Configure EtherChannel
  |
- HRSP v2 IPv6: Packet Tracer Network - HSRP Configuration
- IPCisco.com: ADSL IPv6
- ACLs: Packet Tracer Network - ACLs
- OSPFv3: Networking Academy - IPv6 OSPFv3
- OSPf: Computer Networking - OSPF
- VPN IPsec tunnel (site-to-site): Abdullah Irfan, Medium, VPN tunnel
- VPN site-to-site, IPsec: Gurutech Networking Training - VPN IPsec
- SSH: Sheffer Kimanzi, Configuring ssh
- Telnet: Sheffer Kimanzi, Configuring telnet
- Dynamic NAT: ComputerNetworkingNotes - Dynamic NAT


Thanks!