



MyAdobe

Company

Document Version:

Version 1.2

Author/Position:

Guilherme Fernandes/Network Administrator

Table of Contents

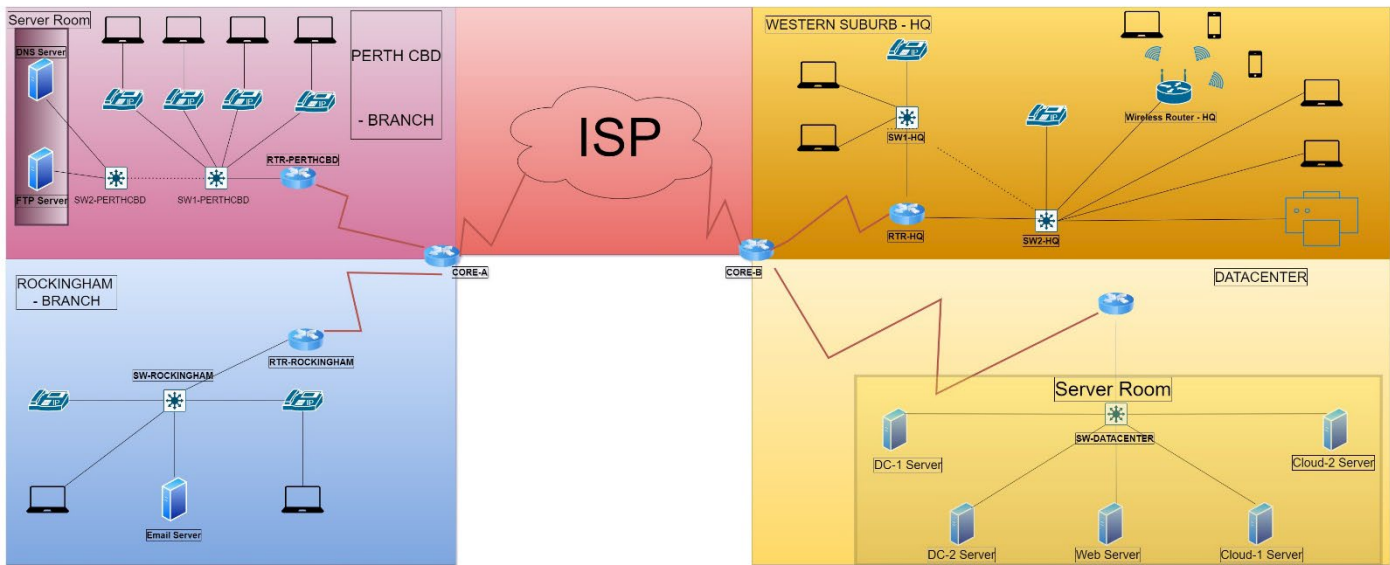
Network Overview	3
Physical Topology	3
Logical Topology	3
Internet Protocol Scheme	4
Networking Scheme	4
IPv4 Addressing Scheme	4
Link Details	6
Equipment used	10
Intermediate Devices	10
End-Devices	11
Configuration steps	11
Email Service	11
FTP Service	12
DNS Service	13
DHCP Service	14
Switch Port Security	15
Test Results of Network	16
Email Results	16
DNS Service	17
DHCP Service	18
FTP Results	19
Switch Port Security Results	20
Ping Results	21
IP phone Results	22
VPN Results	22
Support strategy for the network	23
Recommendations for ongoing management	24
Sign-off	24

Network Overview

Explain the reason behind this document related to My Adobe Company Expansion

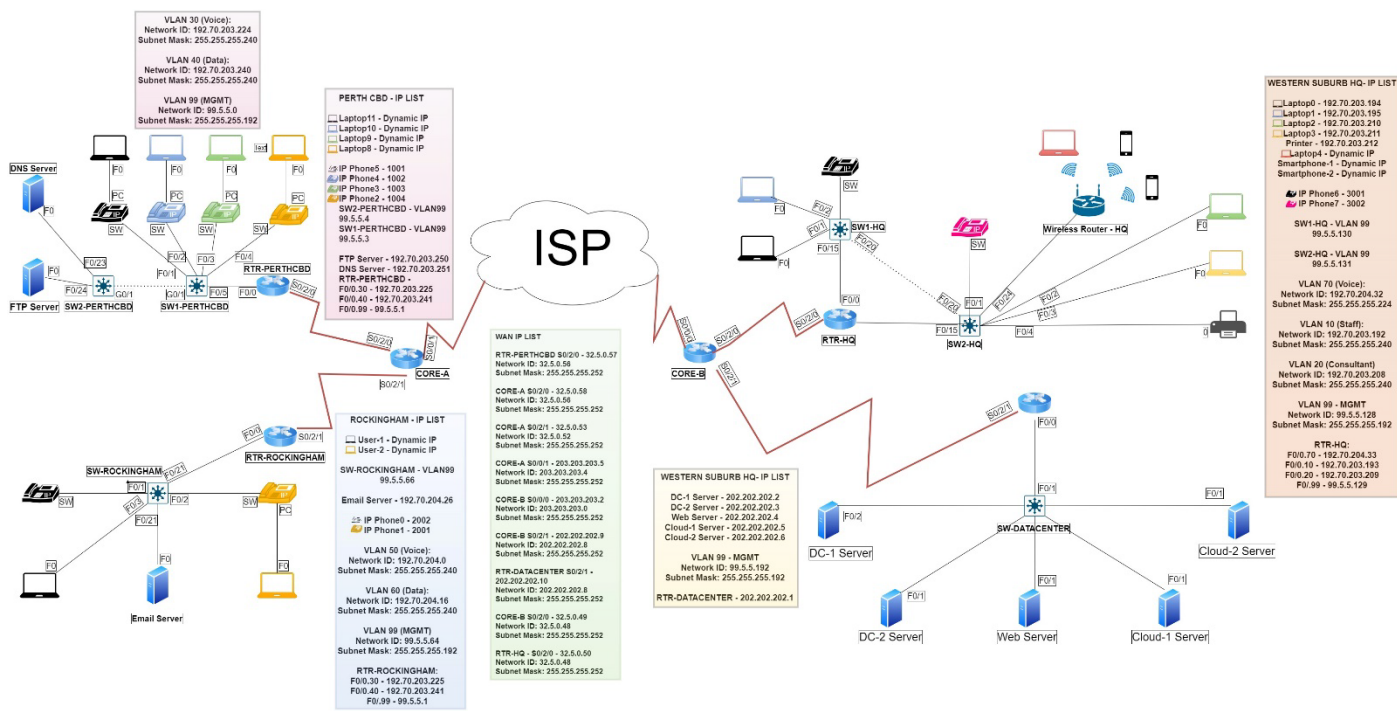
Physical Topology

Below you have a clear draw of the physical topology, dividing every section of the network.



Logical Topology

Under this draw it is easy to check the interfaces that are in use and the IP allocated to them.



Internet Protocol Scheme

The client/server protocol Dynamic Host Configuration Protocol (DHCP) was chosen to supply an Internet Protocol (IP) host with its IP address and other associated configuration information such as the subnet mask and default gateway automatically.

Networking Scheme

A network scheme is crucial to have an organized idea what is the range, subnetmask, name and IP's that can be used.

HQ - LAN

LAN	Network ID	Available Range	Broadcasting ID	Subnetmask
Staff	192.70.203.192	192.70.203.192 - 192.70.203.206	192.70.203.207	255.255.255.240
Consultant	192.70.203.208	192.70.203.209 – 192.70.203.222	192.70.203.223	255.255.255.240
Voice	192.70.204.32	192.70.204.33 - 192.70.204.62	192.70.204.63	255.255.255.240
MGMT	99.5.5.128	99.5.5.129 - 99.5.5.190	99.5.5.191	255.255.255.192

DATACENTER - LAN

LAN	Network ID	Available Range	Broadcasting ID	Subnetmask
MGMT	99.5.5.192	99.5.5.193 - 99.5.5.254	99.5.5.255	255.255.255.192
Default	202.202.202.0	202.202.202.1 – 202.202.202.6	202.202.202.7	255.255.255.248

PERTH CBD - LAN

LAN	Network ID	Available Range	Broadcasting ID	Subnetmask
Voice	192.70.204.0	192.70.204.1 - 192.70.204.14	192.70.204.15	255.255.255.240
Data	192.70.204.16	192.70.204.17 - 192.70.204.30	192.70.204.31	255.255.255.240
MGMT	99.5.5.0	99.5.5.1 - 99.5.5.62	99.5.5.64	255.255.255.192

ROCKINGHAM - LAN

LAN	Network ID	Available Range	Broadcasting ID	Subnetmask
Voice	192.70.204.0	192.70.204.1 - 192.70.204.14	192.70.204.15	255.255.255.240
Data	192.70.204.16	192.70.204.17 - 192.70.204.30	192.70.204.31	255.255.255.240
MGMT	99.5.5.64	99.5.5.65 - 99.5.5.126	99.5.5.127	255.255.255.240

WAN

LAN	Network ID	Available Range	Broadcasting ID	Subnetmask
WAN 1	32.5.0.48	32.5.0.49 - 32.5.0.50	32.5.0.51	255.255.255.252
WAN 2	32.5.0.52	32.5.0.53 - 32.5.0.54	32.5.0.55	255.255.255.252
WAN 3	32.5.0.56	32.5.0.57 - 32.5.0.58	32.5.0.59	255.255.255.252

IPv4 Addressing Scheme

An IP address system is required to uniquely identify a device on an IP network. 32 binary bits make up an IP address. With the use of a subnet mask, these binary bits may be further separated into network and host portions.

HQ - LAN

Device	Interface	IPv4 Address	Subnet Mask	Gateway
RTR-HQ	F0/0.10	192.70.203.193	255.255.255.240	N/A
RTR-HQ	F0/0.70	192.70.204.33	255.255.255.224	N/A
RTR-HQ	F0/0.99	99.5.5.129	255.255.255.192	N/A
RTR-HQ	F0/1.20	192.70.203.209	255.255.255.240	N/A
SW1-HQ	VLAN 99	99.5.5.130	255.255.255.192	99.5.5.129
SW2-HQ	VLAN 99	99.5.5.131	255.255.255.192	99.5.5.129
Laptop0	NIC	192.70.203.194	255.255.255.240	192.70.203.193
Laptop1	NIC	192.70.203.195	255.255.255.240	192.70.203.193
Laptop2	NIC	192.70.203.210	255.255.255.240	192.70.203.209
Laptop3	NIC	192.70.203.211	255.255.255.240	192.70.203.209
Laptop4	NIC	Dynamic IP	255.255.255.192	99.5.5.129
IP Phone7	NIC	Dynamic IP	255.255.255.224	192.70.204.33
IP Phone6	NIC	Dynamic IP	255.255.255.224	192.70.204.33
Smartphone-1	Wireless	Dynamic IP	255.255.255.192	99.5.5.129
Smartphone-2	Wireless	Dynamic IP	255.255.255.192	99.5.5.129
Printer	0	192.70.203.212	255.255.255.240	192.70.203.209

PERTH CBD - LAN

Device	Interface	IPv4 Address	Subnet Mask	Gateway
RTR-PERTHCBD	f0/0.30	192.70.203.225	255.255.255.240	N/A
RTR-PERTHCBD	f0/0.40	192.70.203.241	255.255.255.240	N/A
RTR-PERTHCBD	f0/0.99	99.5.5.1	255.255.255.192	N/A
SW1-PERTHCBD	VLAN 99	99.5.5.3	255.255.255.192	N/A
SW2-PERTHCBD	VLAN 99	99.5.5.4	255.255.255.192	N/A
DNS Server	NIC	192.70.203.251	255.255.255.240	192.70.203.241
FTP Server	NIC	192.70.203.250	255.255.255.240	192.70.203.241
Laptop8	NIC	Dynamic IP	255.255.255.240	192.70.203.241
Laptop9	NIC	Dynamic IP	255.255.255.240	192.70.203.241
Laptop10	NIC	Dynamic IP	255.255.255.240	192.70.203.241
Laptop11	NIC	Dynamic IP	255.255.255.240	192.70.203.241
IP Phone2	NIC	Dynamic IP	255.255.255.240	192.70.203.225
IP Phone3	NIC	Dynamic IP	255.255.255.240	192.70.203.225
IP Phone4	NIC	Dynamic IP	255.255.255.240	192.70.203.225
IP Phone5	NIC	Dynamic IP	255.255.255.240	192.70.203.225

DATACENTER - LAN

Device	Interface	IPv4 Address	Subnet Mask	Gateway
RTR-DATACENTER	F0/0	202.202.202.1	255.255.255.248	N/A

SW-DATACENTER	VLAN 99	99.5.5.194	255.255.255.192	99.5.5.192
DC-1 Server	NIC	202.202.202.2	255.255.255.248	202.202.202.1
DC--2 Server	NIC	202.202.202.3	255.255.255.248	202.202.202.1
WEB Server	NIC	202.202.202.4	255.255.255.248	202.202.202.1
Cloud-1 Server	NIC	202.202.202.5	255.255.255.248	202.202.202.1
Cloud-2 Server	NIC	202.202.202.5	255.255.255.248	202.202.202.1

ROCKINGHAM - LAN

Device	Interface	IPv4 Address	Subnet Mask	Gateway
RTR-ROCKINGHAM	F0/0.50	192.70.204.1	255.255.255.240	N/A
RTR-ROCKINGHAM	F0/0.60	192.70.204.17	255.255.255.240	N/A
RTR-ROCKINGHAM	F0/0.99	99.5.5.65	255.255.255.192	N/A
SW-ROCKINGHAM	F0/20	192.70.204.26	255.255.255.240	192.70.204.17
SW-ROCKINGHAM	VLAN 99	99.5.5.66	255.255.255.192	99.5.5.65
User-1	NIC	Dynamic IP	255.255.255.240	192.70.204.17
User-2	NIC	Dynamic IP	255.255.255.240	192.70.204.17
IP Phone0	NIC	Dynamic IP	255.255.255.240	192.70.204.1
IP Phone1	NIC	Dynamic IP	255.255.255.240	192.70.204.1

WAN

Device	Interface	IPv4 Address	Subnet Mask	Gateway
RTR-PERTHCBD	S0/2/0	32.5.0.57	255.255.255.252	N/A
CORE-A	F0/2/0	32.5.0.58	255.255.255.252	N/A
CORE-A	S0/2/1	32.5.0.53	255.255.255.252	N/A
CORE-A	S0/0/1	203.203.203.5	255.255.255.252	N/A
RTR-ROCKINGHAM	S0/2/1	32.5.0.54	255.255.255.252	N/A
ISP-ROUTER	S0/0/1	203.203.203.6	255.255.255.252	N/A
ISP-ROUTER	S0/0/0	203.203.203.1	255.255.255.252	N/A
CORE-B	S0/0/0	203.203.203.2	255.255.255.252	N/A
CORE-B	S0/2/0	32.5.0.49	255.255.255.252	N/A
CORE-B	S0/2/1	202.202.202.9	255.255.255.252	N/A
RTR-HQ	S0/2/0	32.5.0.50	255.255.255.252	N/A
RTR-DATACENTER	S0/2/1	202.202.202.10	255.255.255.252	N/A

Link Details

Devices were wisely connected to have more efficiency, and linked with proper cables, making sure the speed and safety of the data transmitted is correct.

PERTH CBD - LAN

Source Information				Destination Information	
Switch Name	Port Number	Wall Jack / Port	Location Description	VLAN Description	Security Information
SW2-PERTHCBD	F0/23	NIC	DNS Server	40 - Data	Port Security - Stick 03 – 0060.2FAB.6277 - Violation Shutdown
SW2-PERTHCBD	F0/24	NIC	FTP Server	40 - Data	Port Security - Stick 03 – 00D0.BC38.D62D - Violation Shutdown
SW2-PERTHCBD	G0/1	G0/1	SW1-PERTHCBD	Trunk Link	N/A
SW1-PERTHCBD	G0/1	G0/1	SW2-PERTHCBD	Trunk Link	N/A
SW1-PERTHCBD	F0/1	SW	IP Phone5	30 - Voice	Port Security - Stick 04 – 0090.2141.4535- Violation Shutdown
SW1-PERTHCBD	F0/2	SW	IP Phone4	30 - Voice	Port Security - Stick 04 – 0010.1166.9500 - Violation Shutdown
SW1-PERTHCBD	F0/3	SW	IP Phone3	30 - Voice	Port Security - Stick 04 – 00E0.8FD6.0703 - Violation Shutdown
SW1-PERTHCBD	F0/3	SW	IP Phone2	30 - Voice	Port Security - Stick 04 – 000C.856B.7377 - Violation Shutdown
IP Phone5	PC	F0	Laptop11	40 - Data	Port Security - Stick 04 – 0001.644B.B7B0 - Violation Shutdown
IP Phone4	PC	F0	Laptop10	40 - Data	Port Security - Stick 04 – 000C.CF00.15B7- Violation Shutdown
IP Phone3	PC	F0	Laptop9	40 - Data	Port Security - Stick 04 – 0001.63BC.6309- Violation Shutdown
IP Phone2	PC	F0	Laptop8	40 - Data	Port Security - Stick 04 – 000.0C05.7A56- Violation Shutdown
SW1-PERTHCBD	F0/5	NIC	RTR-PERTHCBD	Trunk Link	N/A
RTR-PERTHCBD	F0/0	NIC	SW1-PERTHCBD	Encapsulation F0/0.30 F0/0.40 F0/0.99	N/A
SW2-PERTHCBD	F0/1-22, G0/2	TBA	TBA	99 – MGMT	Port Security - Shutdown
SW1-PERTHCBD	F0/6-24, G0/2	TBA	TBA	99 - MGMT	Port Security - Shutdown

DATACENTER - LAN

Source Information				Destination Information	
Switch Name	Port Number	Wall Jack / Port	Location Description	VLAN Description	Security Information
RTR-DATACENTER	F0/0	NIC	SW-DATACENTER	N/A	N/A
SW-DATACENTER	F0/1	NIC	RTR-DATACENTER	99 - MGMT	N/A
SW-DATACENTER	F0/2	NIC	DC-1 Server	01 - Default	Port Security - Stick 05 – 0006.2A52.EBAA - Violation Shutdown
SW-DATACENTER	F0/3	NIC	DC-1 Server	01 - Default	Port Security - Stick 05 – 0002.4A89.50B2 - Violation Shutdown
SW-DATACENTER	F0/4	NIC	Web Server	01 - Default	N/A

SW-DATACENTER	F0/5	NIC	Cloud-1 Server	01 - Default	N/A
SW-DATACENTER	F0/6	NIC	Cloud-2 Server	01 - Default	Port Security - Stick 05 – 0060.2F8D.468B - Violation Shutdown/Awn
SW-DATACENTER	F0/7-24, G0/1-2	TBA	TBA	99 - MGMT	Port Security - Shutdown

WESTERN SUBURB HQ - LAN

Source Information				Destination Information	
Switch Name	Port Number	Wall Jack / Port	Location Description	VLAN Description	Security Information
RTR-HQ	F0/1	NIC	SW2-HQ	10 – Staff 20 - Consultant 70 – Voice 99 – MGMT	N/A
RTR-HQ	F0/0	NIC	SW1-HQ	10 – Staff 20 - Consultant 70 – Voice 99 – MGMT	N/A
SW1-HQ	F0/15	NIC	RTR-HQ	Trunk Link	N/A
SW1-HQ	F0/1	NIC	Laptop0	10 - Staff	Port Security - Stick 03 – 0050.0FBC.4163 - Violation Shutdown
SW1-HQ	F0/2	NIC	Laptop1	10 - Staff	Port Security - Stick 03 – 0002.1799.063B - Violation Shutdown
SW1-HQ	F0/3	NIC	IP Phone6	70 – Voice	Port Security - Stick 03 – 0005.5EA0.7083 - Violation Shutdown
SW1-HQ	F0/20	NIC	SW2-HQ	Trunk Link	N/A
SW2-HQ	F0/15	NIC	RTR-HQ	Trunk Link	N/A
SW2-HQ	F0/20	NIC	SW1-HQ	Trunk Link	N/A
SW2-HQ	F0/1	NIC	IP Phone7	70 - Voice	Port Security - Stick 04 –0090.21AE.3D36 – Violation Shutdown
SW2-HQ	F0/2	NIC	Laptop2	20 – Consultant	Port Security - Stick 04 – 00D0.BC42.BBA0 - Violation Shutdown
SW2-HQ	F0/3	NIC	Laptop3	20 – Consultant	Port Security - Stick 04 – 0040.0B39.3C2B - Violation Shutdown
SW2-HQ	F0/4	NIC	Printer	20 – Consultant	Port Security - Stick 04 – 00D0.BCC8.6CB7 - Violation Shutdown
SW2-HQ	F0/24	NIC	Wireless Router – HQ	20 – Consultant	N/A
Wireless Router – HQ	Internet	F0/24	SW2 – HQ	99 – MGMT	N/A
Wireless Router – HQ	Ethernet 0/1	NIC	Laptop4	99 – MGMT	N/A
Wireless Router – HQ	Wireless	Wireless	Smartphone-1	99 - MGMT	N/A
Wireless Router – HQ	Wireless	Wireless	Smartphone-2	99 - MGMT	N/A
Laptop4	NIC	Ethernet 0/1	Wireless Router – HQ	99 - MGMT	N/A

Smartphone-1	Wireless	Wireless	Wireless Router – HQ	99 - MGMT	N/A
Smartphone-2	Wireless	Wireless	Wireless Router – HQ	99 - MGMT	N/A
SW2 – HQ	F0/5-14, F0/16-19, F0/21-23, G0/1-2	TBA	TBA	99 – MGMT	Port Security - Shutdown
SW1 - HQ	F0/4-14, F0/16-19, F0/21-24, G0/1-2	TBA	TBA	99 - MGMT	Port Security - Shutdown

ROCKINGHAM - LAN

Source Information			Destination Information		
Switch Name	Port Number	Wall Jack / Port	Location Description	VLAN Description	Security Information
RTR-ROCKINGHAM	F0/0	NIC	SW-ROCKINGHAM	50 – Voice 60 – Data 99 - MGMT	N/A
SW-ROCKINGHAM	F0/21	NIC	RTR-ROCKINGHAM	Trunk Link	N/A
SW-ROCKINGHAM	F0/1	NIC	IP Phone0	50 - Voice	Port Security - Stick 04 – 0002.1629.A7DC - Violation Shutdown
SW-ROCKINGHAM	F0/2	NIC	IP Phone1	50 - Voice	Port Security - Stick 04 – 0060.2F1E.72C0 - Violation Shutdown
SW-ROCKINGHAM	F0/3	NIC	User-1	60 - Data	Port Security - Stick 04 – 0010.11E3.9925 - Violation Shutdown
SW-ROCKINGHAM	F0/20	NIC	Email Server	60 - Data	Port Security - Stick 04 – 0003.E4E5.7E22 - Violation Shutdown
IP Phone1	PC	NIC	User-2	60 – Data	Port Security - Stick 04 – 0004.9ADC.76DD - Violation Shutdown
SW-ROCKINGHAM	F0/4-19, F0/22-24, G0/1-2	TBA	TBA	99 – MGMT	Port Security - Shutdown

PERTH CBD – CORE A – ROCKINGHAM – ISP - DATACENTER – WESTERN HQ – CORE-B - WAN

Source Information			Destination Information		
Switch Name	Port Number	Wall Jack / Port	Location Description	VLAN Description	Security Information
RTR-PERTHCBD	S0/2/0	NIC	CORE-A	N/A	N/A
CORE-A	S0/2/0	NIC	RTR-PERTHCBD	N/A	N/A
CORE-A	S0/2/1	NIC	RTR-ROCKINGHAM	N/A	N/A
CORE-A	S0/0/1	NIC	ISP-ROUTER	N/A	N/A
ISP-ROUTER	S0/0/0	NIC	CORE-B	N/A	N/A
CORE-B	S0/0/0	NIC	ISP-ROUTER	N/A	N/A

CORE-B	S0/2/1	NIC	RTR-DATACENTER	N/A	N/A
CORE-B	S0/2/0	NIC	RTR-HQ	N/A	N/A
RTR-DATACENTER	S0/2/1	NIC	CORE-B	N/A	N/A
RTR-HQ	S0/2/0	NIC	CORE-B	N/A	N/A

Equipment used

All the equipment used for this network has high-end technology and can provide better services to the company.

Intermediate Devices

All the intermediate devices are high-end, chosen carefully to give high performance and security. Cisco manufactures routers, bridges, frame switches, ATM switches, dial-up access servers, and network administration software, among other networking products.

Devices	Quantity
Router	6
Switch	6

Device Name	Model / PID	System Serial Number	Software Version	Password	Location
SW2-PERTHCBD	WS-C2960-24TT-L	FOC1010X104	Version 15.0(2)SE4; (C2960-LANBASEK9-M)	Console: cisco Enable: cisco	PERTH CBD - BRANCH
SW1-PERTHCBD	WS-C2960-24TT-L	FOC1010X104	Version 15.0(2)SE4; (C2960-LANBASEK9-M)	Console: cisco Enable: cisco	PERTH CBD - BRANCH
RTR-PERTHCBD	JAD05190MTZ	JAD05190MTZ	Version 12.4(15)T1, RELEASE SOFTWARE (fc2); (C2800NM-ADVIPSERVICESK9-M)	Console: cisco Enable: cisco	PERTH CBD - BRANCH
RTR-ROCKINGHAM	JAD05190MTZ	JAD05190MTZ	Version 12.4(15)T1, RELEASE SOFTWARE (fc2); (C2800NM-ADVIPSERVICESK9-M)	Console: cisco Enable: cisco	ROCKINGHAM - BRANCH
SW-ROCKINGHAM	WS-C2960-24TT-L	FOC1010X104	Version 15.0(2)SE4; (C2960-LANBASEK9-M)	Console: cisco Enable: cisco	ROCKINGHAM - BRANCH
SW1-HQ	WS-C2960-24TT-L	FOC1010X104	Version 15.0(2)SE4; (C2960-LANBASEK9-M)	Console: cisco Enable: cisco	WESTERN SUBURB - HQ

SW2-HQ	WS-C2960-24TT-L	FOC1010X104	Version 15.0(2)SE4; (C2960-LANBASEK9-M)	Console: cisco Enable: cisco	WESTERN SUBURB - HQ
RTR-HQ	JAD05190MTZ	JAD05190MTZ	Version 12.4(15)T1, RELEASE SOFTWARE (fc2); (C2800NM-ADVIPSERVICESK9-M)	Console: cisco Enable: cisco	WESTERN SUBURB - HQ
SW-DATACENTER	WS-C2960-24TT-L	FOC1010X104	Version 15.0(2)SE4; (C2960-LANBASEK9-M)	Console: cisco Enable: cisco	WESTERN SUBURB - HQ
RTR-DATACENTER	JAD05190MTZ	JAD05190MTZ	Version 12.4(15)T1, RELEASE SOFTWARE (fc2); (C2800NM-ADVIPSERVICESK9-M)	Console: cisco Enable: cisco	WESTERN SUBURB - HQ

End-Devices

End-user devices are primarily intended to assist our workers with their jobs, data processing, and other workplace processes, as well as to increase workplace efficiency, foster cooperation, and take advantage of new technologies and business advances.

Devices	Quantity
Computer	11
Server	8
IP phone	8
Printer	1

Configuration steps

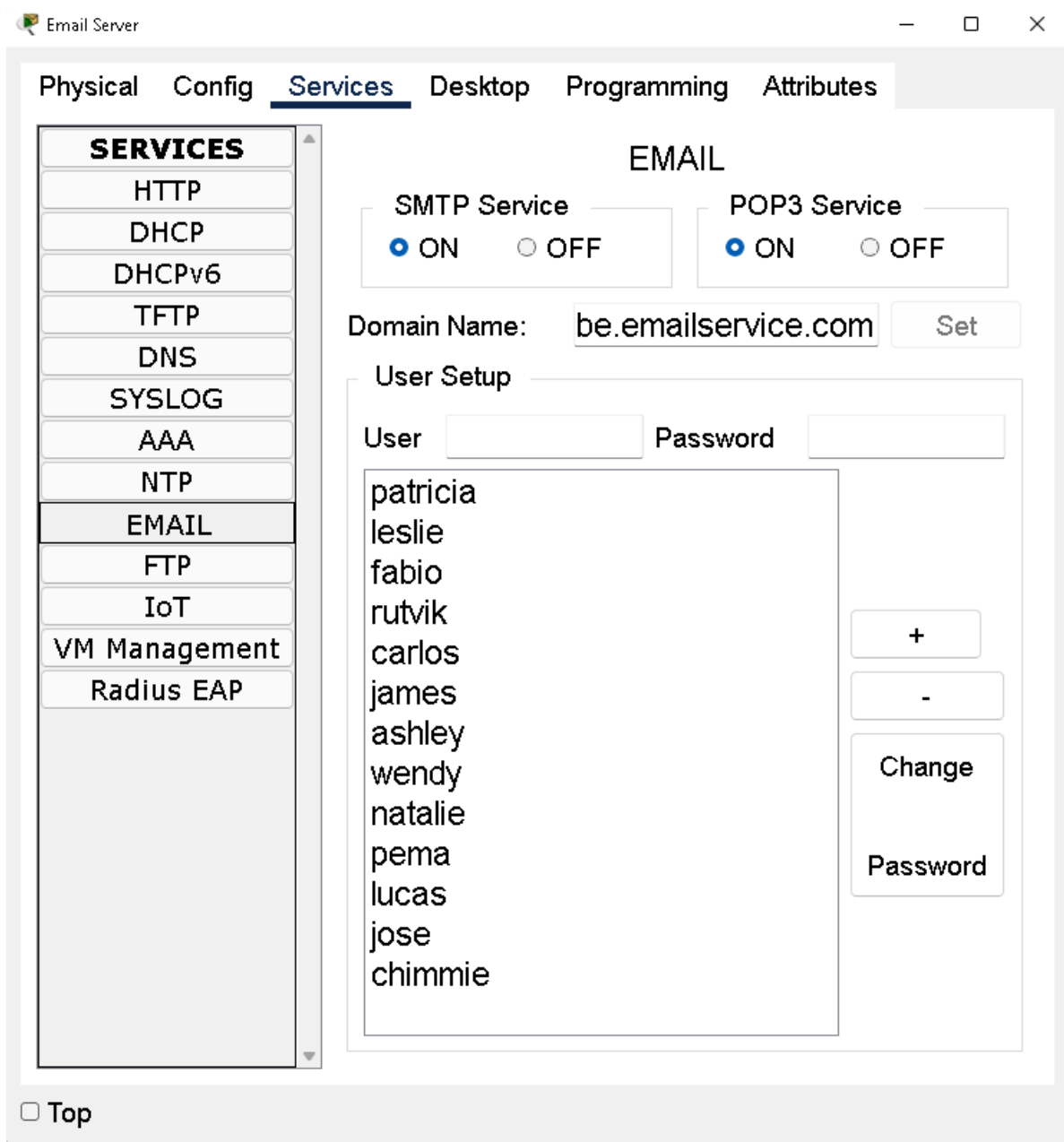
Under this section, you will find steps on how to configure the services below:

- Email Service
- FTP Service
- DNS Service
- DHCP Service
- Switch port security

Email Service

It allows us to send and receive messages, mail, and crucial information within the organization.

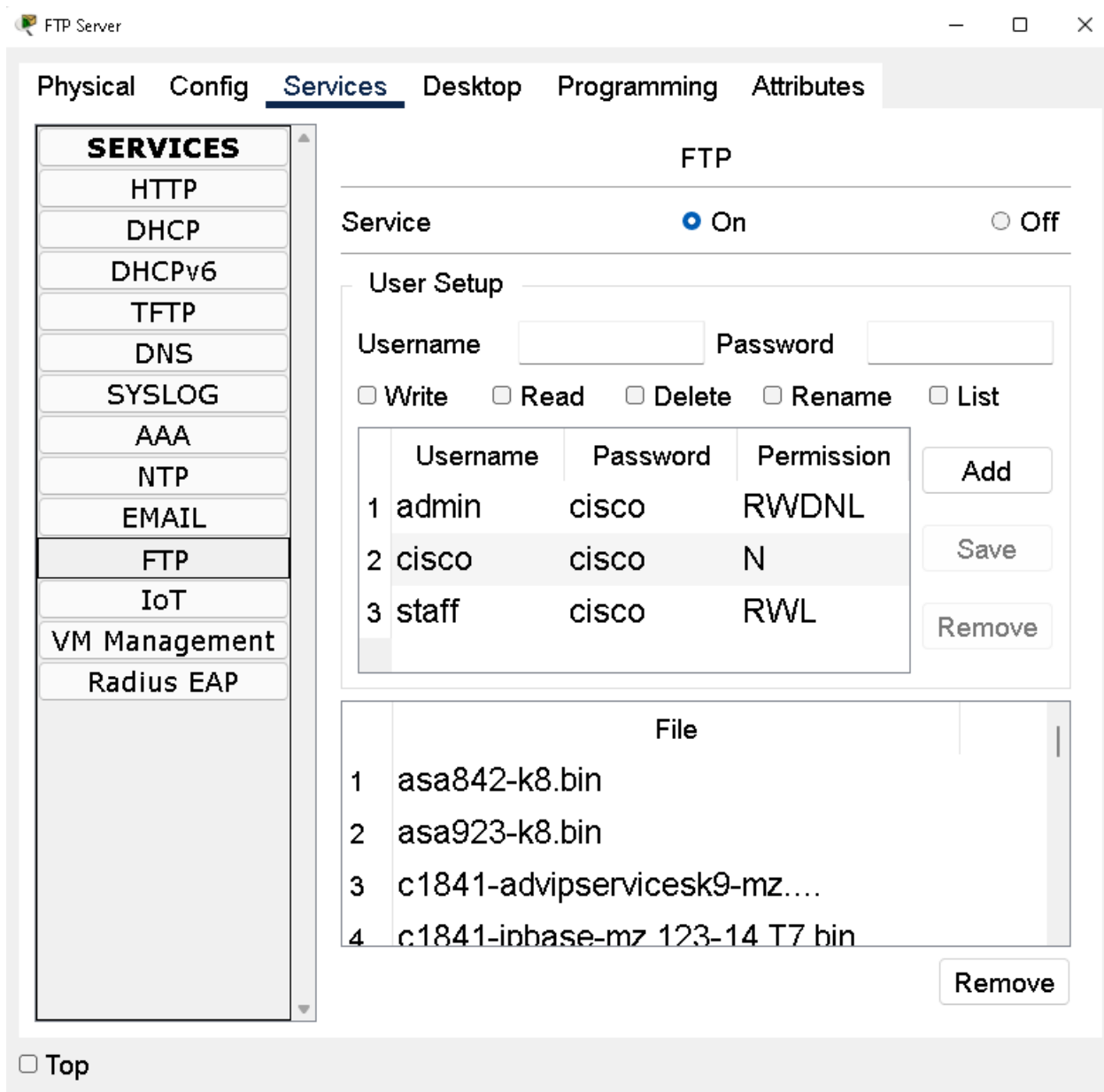
To configure this service, you will need to first access your Email Server and disable every other service that are not related to Email. Next, by clicking on the EMAIL tab, make sure that SMTP and POP3 Service are on. Your domain name must be the same as you created on the DNS server, in this case, myadobe.emailservice.com. Lastly, create users for every device that can send and receive emails, applying the standard password: cisco.



FTP Service

FTP allows you to send and receive files between computers or over the internet between sites. To maintain websites, FTP is a must-have technology in the company.

To configure this service, you will need to first access your FTP Server and disable every other service that are not related to FTP. Make sure the service is turned ON and follow the configuration. As default, username: cisco password: cisco cannot be deleted on packet tracer but can be modified. By creating other users, we can address what they and what they cannot do. Also, make sure that you create a resource record under the DNS Service, which in this case is myadobe.ftpservice.



DNS Service

DNS guarantees that the internet is not only user-friendly, but also runs smoothly, swiftly, and effectively loading whatever material we want. As the company is growing and introducing more devices, it is much easier to access the internet without being stuck and memorizing long lists of numbers (IP addresses) to access the content we want. To configure this service, you will need to first access your DNS Server and disable every other service that is not related to DNS. Make sure the service is turned ON and follow the configuration. By adding all services as required, such as email, FPP, and web, always checking if the IP addresses are correct, you are good to go.

DNS Server

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type **A Record** ▼

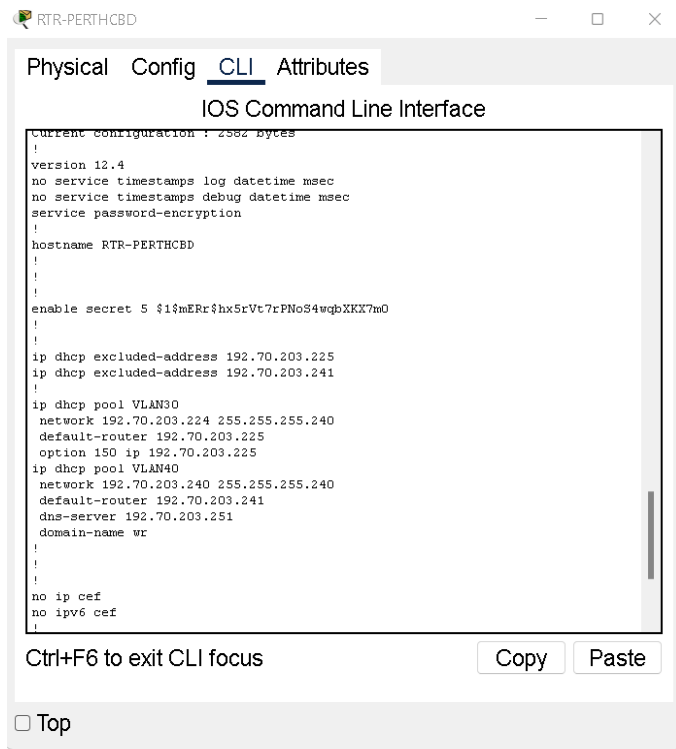
Address

No.	Name	Type	Detail
0	myadobe.com	A Record	202.202.202.4
1	myadobe.emails...	A Record	192.70.204.26
2	myadobe.ftpserv...	A Record	192.70.203.250
3	www.myadobe.com	A Record	202.202.202.4

☐ Top

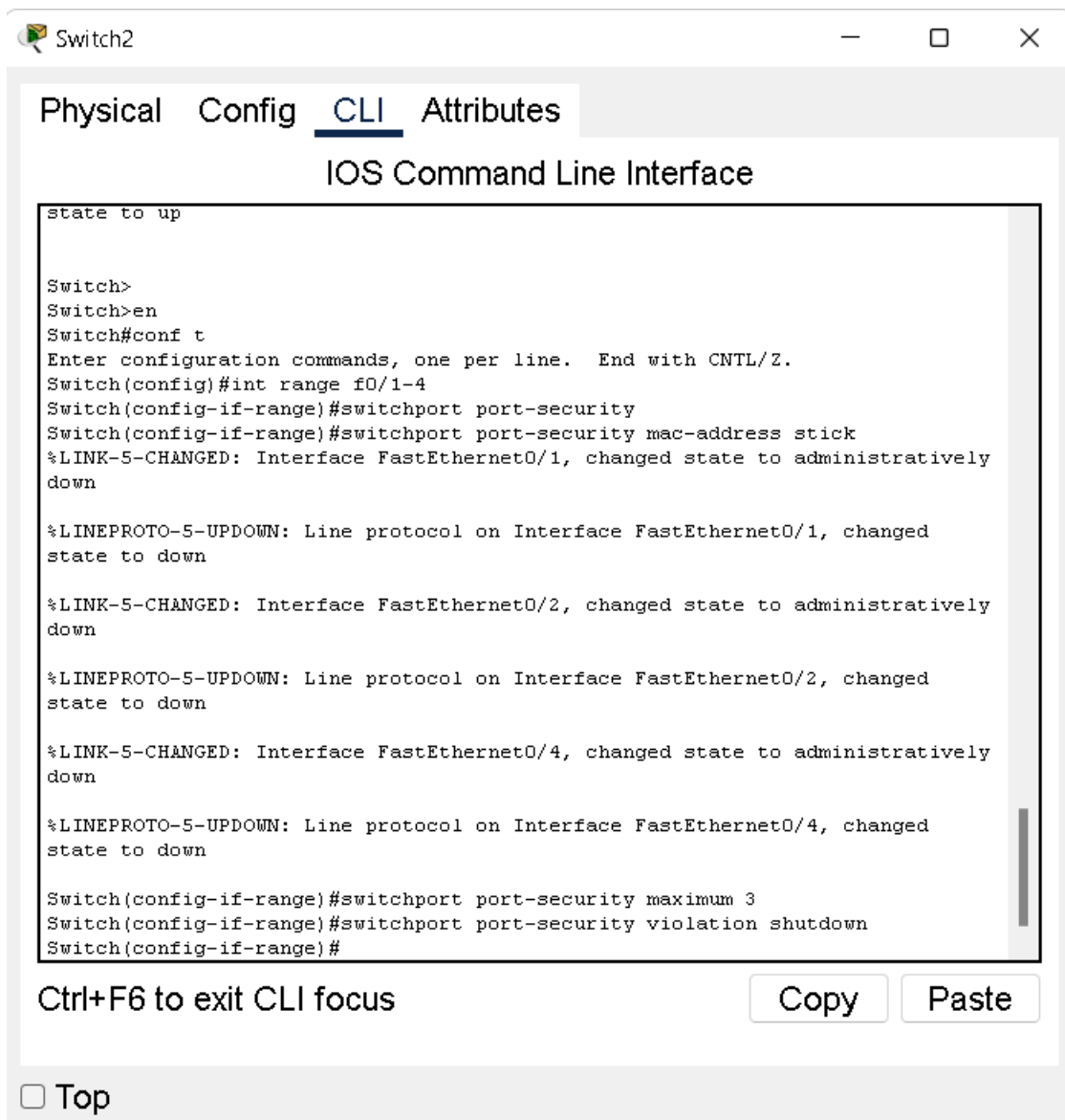
DHCP Service

When IP addresses are given manually, DHCP minimises the probability of frequent mistakes. It also guarantees that no two hosts have the same IP address. Because more and more devices are being added, our company must have dynamic IP for some devices to make sure it does not repeat.



Switch Port Security

The switchport security feature (Port Security) is a key part of the network switch security jigsaw in our company because it allows you to control which addresses are authorised to send traffic on switchports inside the switched network.

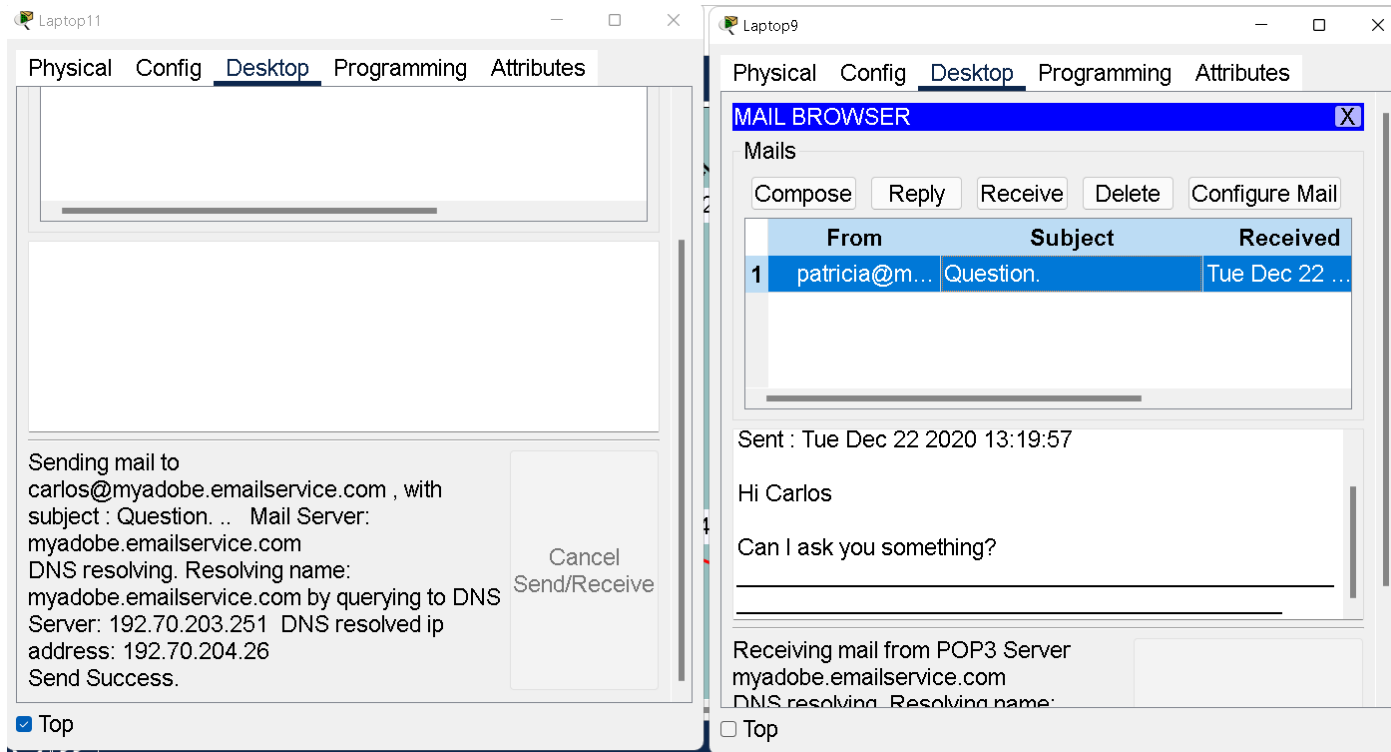


Test Results of Network

Troubleshooting and testing are crucial to check if every configuration is working. As our company needs communication, all the services must be operating as requested.

Email Results

Email service is configured and working as requested, being able to send email throughout the network and other sites. This is an example of Patricia sending an email to Carlos.



DNS Service

Under our DNS Server, a website name is configured, and the content under the Web Server, making it possible to access using myadobe.com instead of the IP address designated to it.



DHCP Service

On the example below, you can see that the request for a dynamic IP is successful and ready to operate. It is important to our company to have different IP addresses within the devices to do not have any conflict.

Laptop8

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address 192.70.203.244

Subnet Mask 255.255.255.240

Default Gateway 192.70.203.241

DNS Server 192.70.203.251

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::20C:85FF:FE6B:7377

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

☐ Top

FTP Results

Tests were performed to check if users can or cannot access, list, remove, rename, and read files. Separate users are crucial to have a secure environment in the company.

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.70.203.250
Trying to connect...192.70.203.250
Connected to 192.70.203.250
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.70.203.250:
%Error ftp://192.70.203.250/ (No such file or directory Or Permission denied)
550-Requested action not taken. permission denied).

ftp>mkdir home
Invalid or non supported command.
ftp>

C:\>ftp 192.70.203.250
Trying to connect...192.70.203.250
Connected to 192.70.203.250
220- Welcome to PT Ftp server
Username:admin
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.70.203.250:
0 : asa842-k8.bin 5571584
1 : asa923-k8.bin 30468096
2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
3 : c1841-ipbase-mz.123-14.T7.bin 13832032
4 : c1841-ipbasek9-mz.124-12.bin 16599160
5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
7 : c2600-i-mz.122-28.bin 5571584
8 : c2600-ipbasek9-mz.124-8.bin 13169700
9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin 5571584
12 : c2800nm-ipbasek9-mz.124-8.bin 15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin 3058048
15 : c2950-i6q412-mz.121-22.EA8.bin 3117390
16 : c2960-lanbase-mz.122-25.FX.bin 4414921
```

Switch Port Security Results

By running the command “do show port-security”, it is possible to check which port are added to the switch port security and manage them.

SW2-PERTHCBD
—
□
×

Physical
Config
CLI
Attributes

IOS Command Line Interface

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed
state to up

Unauthorised Access is Prohibited!

User Access Verification

Password:
SW2-PERTHCBD>enable
Password:
Password:
SW2-PERTHCBD#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW2-PERTHCBD(config)#interface FastEthernet0/6
SW2-PERTHCBD(config-if)#ex
SW2-PERTHCBD(config)#do sh port
SW2-PERTHCBD(config)#do sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)        (Count)        (Count)
-----
Fa0/23        3            1              0             Shutdown
Fa0/24        3            1              0             Shutdown
-----
SW2-PERTHCBD(config)#

```

Ctrl+F6 to exit CLI focus

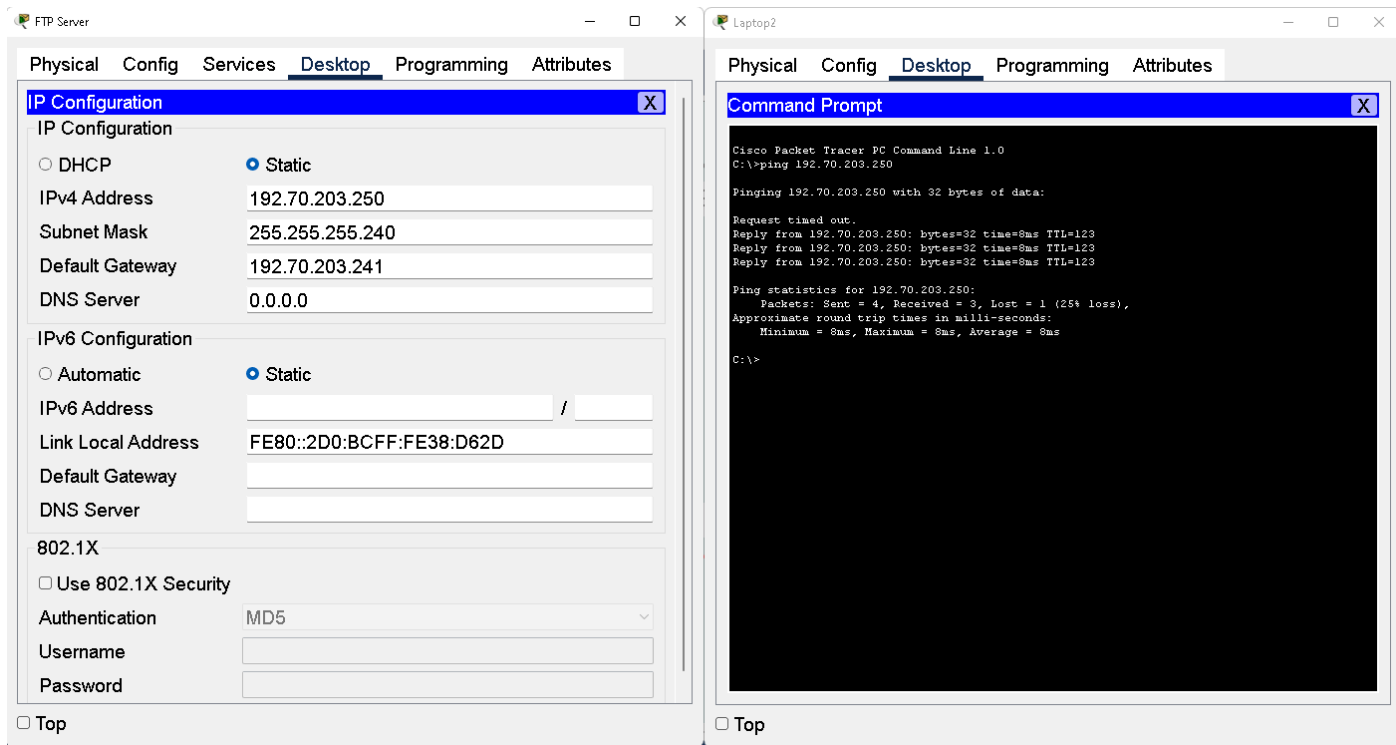
Copy

Paste

☐ Top

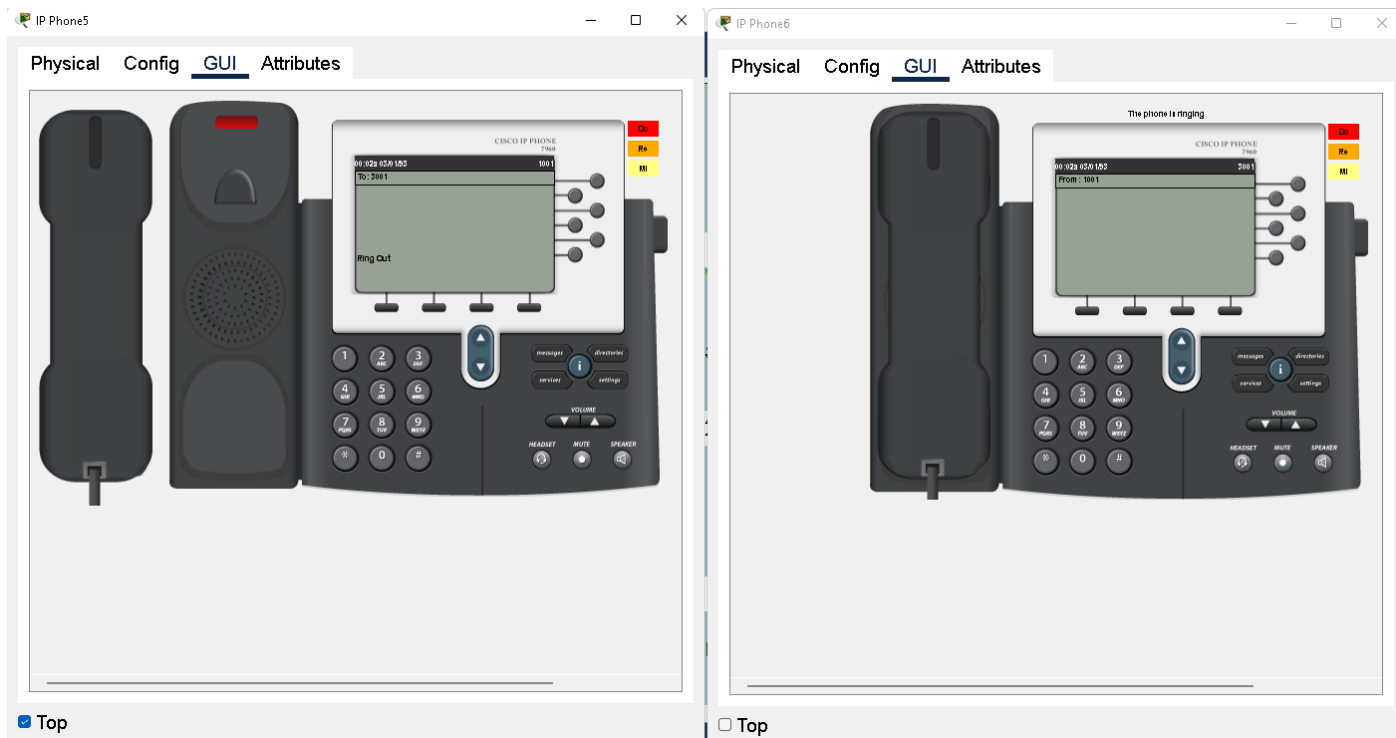
Ping Results

All devices must interact to each other, and to test that, a simple ping test is necessary to check if you can connect to other devices.




IP phone Results

As we are always communicating to each other, typing might be a bit tricky and not fast enough when we need the information. Because of that, telephones were implemented to the company, but also configured to be voIP telephones, which means that is cheaper than regular telephones.



VPN Results

As we want to keep our data safe, a VPN is required to encrypt the data between the routers. A test were done and packets were encrypted, assuring the safety of the data from point A to point B.

 RTR-DATACENTER

Physical Config CLI Attributes

```
outbound pcp sas:

local ident (addr/mask/prot/port): (202.202.202.0/255.255.255.248/0/0)
remote ident (addr/mask/prot/port): (192.70.203.208/255.255.255.240/0/0)
current_peer 202.202.202.9 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 202.202.202.10, remote crypto endpt.: 202.202.202.9
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/2/1
current outbound spi: 0x58919A82(1485937282)

inbound esp sas:
  spi: 0xF5689998(4117272984)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2002, flow_id: FPCA:1, crypto map: VPN-MAP
    sa timing: remaining key lifetime (k/sec): (4525504/3543)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x58919A82(1485937282)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2003, flow_id: FPCA:1, crypto map: VPN-MAP
    sa timing: remaining key lifetime (k/sec): (4525504/3543)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

outbound ah sas:

outbound pcp sas:

local ident (addr/mask/prot/port): (202.202.202.0/255.255.255.248/0/0)
remote ident (addr/mask/prot/port): (192.70.203.240/255.255.255.240/0/0)
current_peer 202.202.202.9 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 202.202.202.10, remote crypto endpt.: 202.202.202.9
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/2/1
current outbound spi: 0x7F6F16B5(2137986741)
```

Ctrl+F6 to exit CLI focus

☐ Top

Support strategy for the network

Before building a network, it is important to have a previous strategy to do not fail or have issues during the configuration. Creating or joining a network has costs: time, money, energy, and other precious resources that could

be spent elsewhere. The network's structure and kind, membership and governance styles, timing, goal, and other aspects are all considered in our plan. They can assist to build a comprehensive plan of action for your network's particular background, history, and ambitions when used together.

Recommendations for ongoing management

- Make a list of the systems that are most essential to you.
- Create a change management strategy.
- Be aware of the requirements for compliance. Recognize what you need to track and for how long.
- Remember to keep an eye on your network's perimeter. Keep an eye on what's coming in and out.

Sign-off

Signature	
Name	Guilherme Fernandes
Position	Network Administrator
Date	01/05/2022

Signature	<i>John Adams</i>
Name	John Adams
Position	Operation Manager
Date	01/05/2022