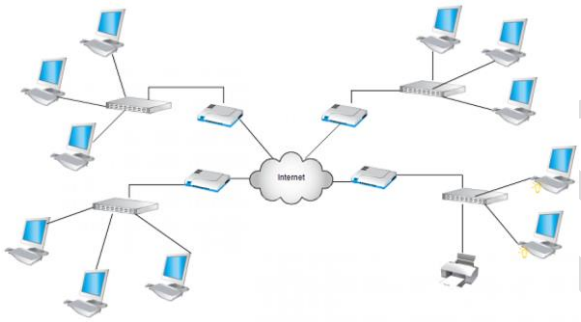
Pacific IT Solutions
2/246 Varsity Parade,
Varsity Lake, Gold Coast,
QLD 4227
Tel. 0431616438

Daniel Cortez



Network Description

WESTERN MINING 2020

This document will present a detailed description of all the requirements proposed by Pacific IT Solutions regarding security and wan connection functionality

FOR THE KNOWLEDGE OF OUR CLIENT:

Network Description

For the construction of our network in the new Brisbane office, we thought it appropriate to use the maximum capacity of the devices. That is why we reduced to the maximum the amount of elements necessary to fulfill their functions more efficiently in addition to reducing their cost to the maximum.

Router:

The first thing we will need is a Cisco 2811 router in order to be able to properly connect Brisbane with Head Office and have another interface enabled so that all devices have internet access. We will call this Router R-Brisbane.

To R-Brisbane we connect a HWIC-1GE-SFP connector to have the possibility of having a gigabit interface in the event of needing a high-speed port in case of any problem that may arise because we will occupy the other interfaces that are available.

In addition, we will integrate a HWIC-2T connector that will give us the possibility of having two serial interfaces that will be essential for wan routing.

Switches:

We consider switches as a fundamental part of our network. It will allow us to connect our devices correctly, giving us the opportunity to configure different vlans, in order to separate and manage the departments of the office.

The model to use is the 2960 switch and we will use five of these, one for each department plus a main switch where they will all connect.

The main switch will be configured so that all vlans connected to it are transported to R-brisbane. We will explain the design of these configurations later.

Devices:

Regarding the devices and end-devices required, in our network example in Packet Tracer we have configured two hosts and a server per department respectively (it is assumed that the department should have 48 PCs and one server per department, but for purposes design quantity was reduced).

All the IP addresses of each device were dynamically configured which we will explain in detail in the configuration section.

Cabling:

To connect our devices we have chosen two types of wires: Cooper Cross-Over and Cooper Straight Through.

We connect from host and server to the switch with Cooper Straight Through cable which has the code T568a or T568b on both ends in the RJ-45 connector for a better adaptation. The communication between the Mainswitch and R-brisbane was also through this cable.

At the same time we will use the Cooper Straight Through cable for the connection between the switches of the four departments to the Mainswitch since we need the RJ-45 connectors with their models T568A at one end and T568 at the other end in case we want to use communication in Fullduplex.

Configuration

To begin to detail our internal configuration, we start with the with the ip address scheme by department

Ip address scheme:

The client asked us for the 172.16.0.0 scheme for private IP addresses, therefore we configure the subnets with the vlsm model as follows:

Network	Size	Cns	Net IP	1st available	Last available	Broadcast IP	Subnetmask
Sales	510	512	172.16.0.0 /23	172.16.0.1	172.16.1.254	172.16.1.255	255.255.254.0
Operations	510	512	172.16.2.0 /23	172.16.2.1	172.16.3.254	172.16.3.255	255.255.254.0
Managements	510	512	172.16.4.0 /23	172.16.4.1	172.16.5.254	172.16.5.255	255.255.254.0
Exploration	510	512	172.16.6.0 /23	172.16.6.1	172.16.7.254	172.16.7.255	255.255.254.0
Cities	2	4	172.16.8.0 /30	172.16.8.1	172.16.8.2	172.16.8.3	255.255.255.252

Clearly this scheme will satisfy the amount of staff required by department in addition to giving us an IP range for the addresses between both offices.

Dynamic Ip Addressing:

The requirement has been clear, the IP addresses of the devices must be dynamically assigned and therefore we will explain the detail of the configuration in R-Brisbane to achieve this requirement:

We have configured a pool per department to indicate the dynamic range that will be used to assign the IP addresses in consecutive order starting with the tenth, available in each network. The name of the pool is the same name of the department.

The configuration is as follows:

CONFIGURATION EXCLUDED-ADDRESS	RANGE
ip dhcp excluded-address	172.16.0.1 172.16.0.9
ip dhcp excluded-address	172.16.2.1 172.16.2.9
ip dhcp excluded-address	172.16.4.1 172.16.4.9
ip dhcp excluded-address	172.16.6.1 172.16.6.9

ip dhcp pool SALES
network 172.16.0.0 255.255.254.0
default-router 172.16.0.1

ip dhcp pool OPERATIONS
network 172.16.2.0 255.255.254.0
default-router 172.16.2.1

ip dhcp pool MANAGEMENT
network 172.16.4.0 255.255.254.0
default-router 172.16.4.1

ip dhcp pool EXPLORATION
network 172.16.6.0 255.255.254.0
default-router 172.16.6.1

Remote login:

We have also been asked in a very important way to be able to have remote access to all the switches and routers in the Brisbane office. For this, we have designed and configured all the remote accesses enabling the pertinent passwords to the VTY lines in addition to assigning addresses to the vlans and enabling the default gateway function in order to have free access to the devices.

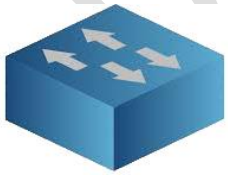
In the following table we will detail each step of the configuration:

As a bonus, we have configured the console password to have direct control if we want to access the device from an additional computer.

Passwords must respect capitals and lowercase characters.

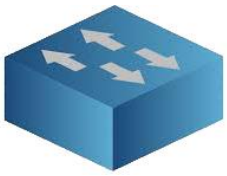
SWITCH SALES	***VLAN 2***	***172.16.0.0***
Console Password	xxxx	
VTY Password	xxxx	
Interface Vlan	172.16.0.2	
Default-Gateway	172.16.0.1	
Password Device	xxxx	

SWITCH OPERATIONS	***VLAN 3***	***172.16.2.0***
Console Password	xxxx	
VTY Password	xxxx	
Interface Vlan	172.16.2.2	
Default-Gateway	172.16.2.1	
Password Device	xxxx	



SWITCH MANAGEMENT	***VLAN 4***	***172.16.4.0***
Console Password	xxxx	
VTY Password	xxxx	
Interface Vlan	172.16.4.2	
Default-Gateway	172.16.4.1	
Password Device	xxxx	

SWITCH EXPLORATION	*VLAN 5*	*172.16.6.0*
Console Password	xxxx	
VTY Password	xxxx	
Interface Vlan	172.16.6.2	
Default-Gateway	172.16.6.1	
Password Device	xxxx	



SWITCH MAINSWITCH	*VLAN 2-3-4-5*
Console Password	xxxx
VTY Password	xxxx
Interface Vlan	172.16.0.3
Default-Gateway	172.16.0.1
Password Device	xxxx

ROUTER R-BRISBANE	*INTERFACES*
Console Password	xxxx
VTY Password	xxxx
Interfaces	FaEth 0/0-0/0.20-0/0.30 0/0.40-0/0.50 Serial 0/2/0 , 0/2/1
Password Device	xxxx

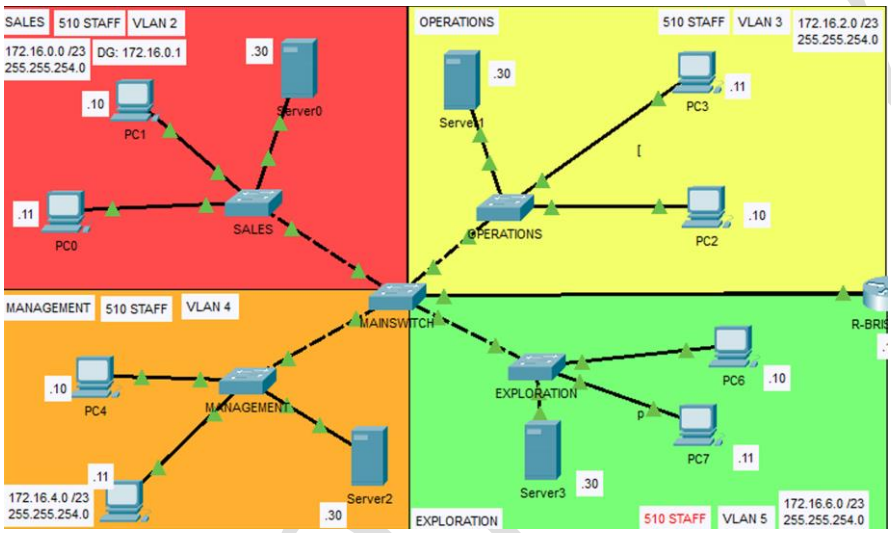
If someone tries to access via Telnet from the Head Office in Sydney, they will be accepted with the above settings.

Vlans Configuration:

In order to make the most of the resources we have at our disposal, we have come to the conclusion that in order to have a better management and a better traffic flow between the office devices, we will set up and manage a network to four different networks (one by department with the vlans function.

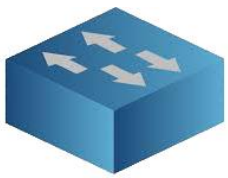
As we know, the vlan function allows us to divide a switch and assign interfaces to each of them for better control.

As we previously reported, we have five switches, four for the departments and one as a main switch where the four networks to be used will converge, as explained in the following graph:

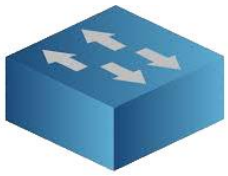


Next, we will detail the vlan configuration of each switch, both in access mode and in trunk mode.

SWITCH	*VLAN (NAME)*	*INTERFACES*
SALES	1 (Default)	Fa 0/1
	2 (SALES)	Range Fa0/2-Fa0/24 Gig 0/1-Gig 0/2



SWITCH	*VLAN (NAME)*	*INTERFACES*
OPERATIONS	1 (Default)	Fa 0/1
	3 (OPERATIONS)	Range Fa0/2-Fa0/24 Gig 0/1-Gig 0/2



SWITCH	VLAN (NAME)	INTERFACES
MANAGEMENT	1 (Default)	Fa 0/1
	4 (MANAGEMENT)	Range Fa0/2-Fa0/24 Gig 0/1-Gig 0/2

SWITCH	VLAN (NAME)	INTERFACES
EXPLORATION	1 (Default)	Fa 0/1
	5 (EXPLORATION)	Range Fa0/2-Fa0/24 Gig 0/1-Gig 0/2

SWITCH	VLAN (NAME)	INTERFACES
MAINSWITCH	1 (Default)	Range Fa 0/1-Fa0/19 Gig 0/1-Gig0/2
	2 (SALES)	Fa 0/22
	3 (OPERATIONS)	Fa 0/21
	4 (MANAGEMENT)	Fa 0/23
	5 (EXPLORATION)	Fa 0/20
TRUNK MODE		Fa 0/24

Inter Vlan Configuration:

So that all the devices and switches have communication with each other (since due to the vlan configuration they should not communicate) we have configured an interface of the R-brisbane router Fa0/0 in such a way that it is divided into 4 subinterfaces with the corresponding encapsulation so that the vlans can exchange traffic without problems.

We will explain it as follows:

Fa 0/0

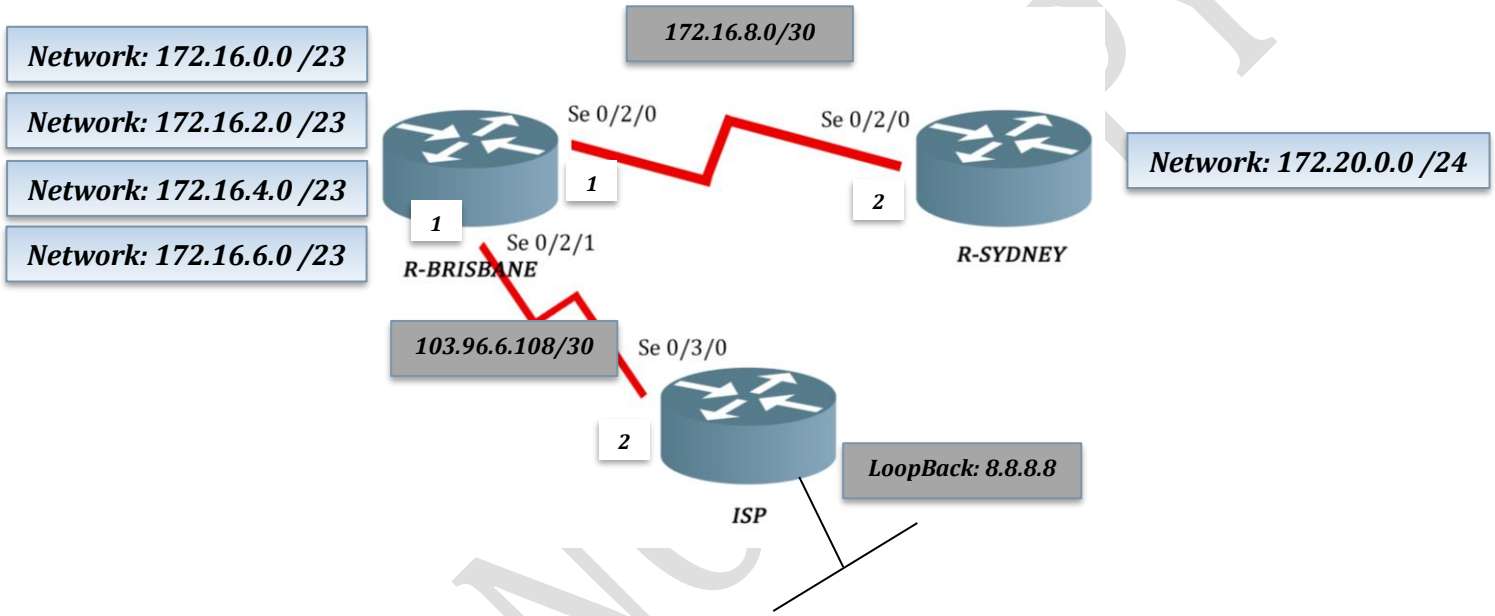
INT FA 0/0.20	INT FA 0/0.30	INT FA 0/0.40	INT FA 0/0.50
Encapsulation dot1q 2	Encapsulation dot1q 3	Encapsulation dot1q 4	Encapsulation dot1q 5
Ip 172.16.0.1	Ip 172.16.2.1	Ip 172.16.4.1	Ip 172.16.6.1
255.255.254.0	255.255.254.0	255.255.254.0	255.255.254.0

Wan Configuration:

The Western Mining company has informed us that the communication and connection between both offices will be standardized under the ospf (Open Shortest Path First) protocol as well as the link that will allow both networks to have full access to the internet.

In the next section we will detail the programmed configuration of both the Brisbane office router (R-brisbane) and the Sydney Head office (R-sydney).

This is the design chosen for the ospf configuration between the routers involved:



The ospf protocol was configured under the name of Router ospf 1 area 0 in each router as well as the adjacent networks that correspond to each one. In the next box we will go on to detail which are the adjacent networks, the passive interfaces and all the information corresponding to the ospf configuration.

OSPF	AREA	ROUTER	ADJACENT NETWORKS	WILDCARD	PASSIVE INTERFACES
1	0	R-BRISBANE	Network 172.16.0.0 Network 172.16.2.0 Network 172.16.4.0 Network 172.16.6.0 Network 172.16.8.0 Network 103.96.6.108	0.0.1.255 0.0.1.255 0.0.1.255 0.0.1.255 0.0.0.3 0.0.0.3	Fa 0/0.20 Fa 0/0.30 Fa 0/0.40 Fa 0/0.50
1	0	R-SYDNEY	Network 172.20.0.0 Network 172.16.8.0	0.0.0.255 0.0.0.3	Fa 0/0
1	0	ISP	Network 103.96.6.108 Network 8.8.8.8	0.0.0.3 0.0.0.0	

NAT Configuration:

Western mining was precise and concise in asking us that all devices both Brisbane and Sydney must have full access to the internet.

As could be seen previously, in our simulation in Cisco Packet Tracer we have implemented a third router called ISP, which will help us to represent any web page or some type of request that is sent from our devices within the network.

As we already know, the ip addresses of each of the devices is private, therefore we must configure an inside global ip address, in order to establish a connection with the isp router (internet) and that the addresses remain private.

Our network consists of many addresses where users will make constant connections to the internet, so we have decided to configure a Nat translation under the Pat (Port Address Translation) model, which will allow us to map or translate all private internal IP addresses to a single one public where only the port will change.

In this case we have decided to configure the interface Se 0/2/1 of R-Brisbane router and its IP address as the public IP address that will send us out to the isp Router.

It is also worth saying that we have configured a loopback interface within the isp router with the address 8.8.8.8 0.0.0.0 which in this case will simulate a web page and will also allow us to connect and verify ping from the network, which will indicate precisely that the configuration has been done in the correct way.

In the next box we go on to detail the internal configuration of each router with respect to the Nat.

ROUTER	*ACCESS-LIST*	*NAT CONFIG*
R-Brisbane	ACL 1 permit-any	ip nat inside source list 1 interface Serial0/2/1 overload

In this way, the translation will be feasible, next we will demonstrate it by pinging from the device 172.16.0.11 to the loopback interface 8.8.8.8. The translation is as follows:

PRO	*INSIDE GLOBAL*	*INSIDE LOCAL*	*OUTSIDE LOCAL*	*OUTSIDE GLOBAL*
icmp	103.96.6.109:6	172.16.0.11:6	8.8.8.8:6	8.8.8.8:6
icmp	103.96.6.109:7	172.16.0.11:7	8.8.8.8:7	8.8.8.8:7
icmp	103.96.6.109:8	172.16.0.11:8	8.8.8.8:8	8.8.8.8:8
icmp	103.96.6.109:9	172.16.0.11:9	8.8.8.8:9	8.8.8.8:9

Security

There are very important elements in building a network such as efficiency, reliability, scalability. But one of the most important is security. Of course we do not want the network to be vulnerable to any type of attack, intrusion or any hole that allows the incorrect functionality of the network.

Some conditions have been required of us for security. The main one is that none of the three departments in the Brisbane office (Sales, Operations and Explorations) can have access to the server in the Management department. In turn, all the devices of the Management department, including the server, must have access to the other departments including full internet access.

We have decided that the best way to achieve this requirement is to configure in R-brisbane, an access list with two indications that we will detail below:

ROUTER R-BRISBANE	
Access list 100 (extended)	deny icmp any host 172.16.4.30 echo
Access list 100 (extended)	permit ip any 172.16.4.0 0.0.1.255

It is worth mentioning that in terms of security we have configured passwords for each device in the Brisbane network, both in its console mode and in the device's own password, in addition to its encryption and the corresponding banner so that each element is re-configured or pre-configured determined by the person who has the relevant services:

BANNER	***UNAUTHORIZED ACCESS IS STRICTLY PROHIBITED***