(TASK 1) Description of Requirements:

WESTERN MINING 2020

This document will present a detailed description of all the requirements proposed by Pacific IT Solutions for the implementation and distribution of a quality and safe network, in its new office in Brisbane.

FOR THE KNOWLEDGE OF OUR CLIENT:

To consider:

We must take into account and consider that the services of this new network in the new office located in Brisbane, will initially be occupied by a small staff, but that in the future it could increase rapidly. Therefore, we must consider a total of 510 staff connected by department.

Departments

The new Brisbane office will have 4 departments: Sales, Operations, Management and Exploration.

Security requirements

Western Mining has asked us as a security protocol that the Management department´s server should not be accessible from the other 3 departments (Sales, Operations and Exploration).

But likewise, all the staff of the Management department must have full access to the networks of the other 3 departments without exception. In addition to that all devices, both as hosts and servers, must have full access and connectivity to the internet.

It should also be taken into consideration that in the future the Head Office in Sydney could change to use a Non-Cisco router.

OTHER REQUIREMENTS

Since the Head Office in Sydney uses the ip address 172.20.0.0 for all its staff, the Brisbane office requires to use the 172.16.0.0 network for its four departments.

It is required to review and check the sparkies for power and data, to ensure that the cabling and all the devices conform to the network design.

Develop and design a network proposal with all the costs that it needs to be carried out.

As for the routers, these must be the Cisco 2811 model, the switches must be 2960. The central office requires remote access to the routers and switches. IP addresses must be dynamically configured. 48 PCs and 1 server per department must be considered in addition to the cables and connectors that are necessary. In addition, the configuration between both offices must be under the ospf protocol.

Finally, consider that our client has in mind for the near future to transform his network to a wireless design, so we were required to complete a wireless site survey while we carry out our network design.

(TASK 2) 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	

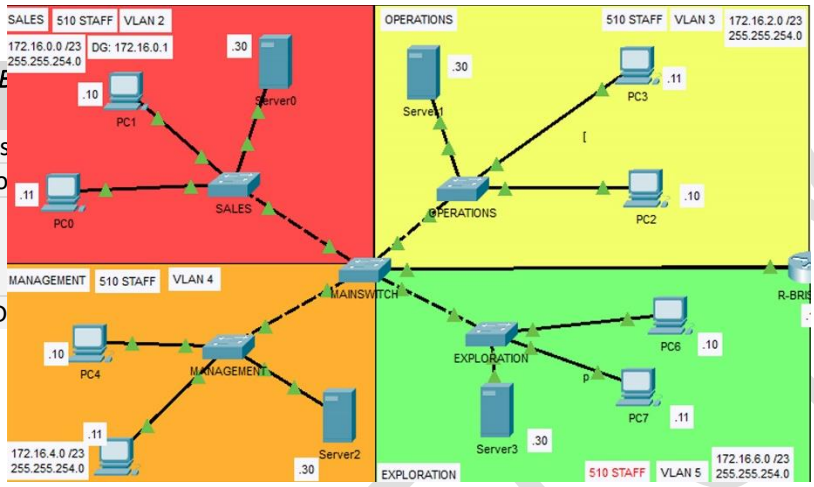
SWITCH MANAGEMENT	*VLAN 4*	*172.16.4.0*
Console Password	xxxx	
VTY Password	xxxx	
Interface Vlan	172.16.4.2	
Default-Gateway	172.16.4.1	
Password Device	xxxx	

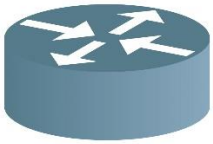
SWITCH EXPLORATION	*VLAN 5*	*172.16.6.0*
Console Password	xxxx	
VTY Password	xxxx	
Interface Vlan	172.16.6.2	
Default-Gateway	172.16.6.1	
Password Device	xxxx	

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-E	
Console Pas	
VTY Passwo	
Interfaces	
Password D	





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:

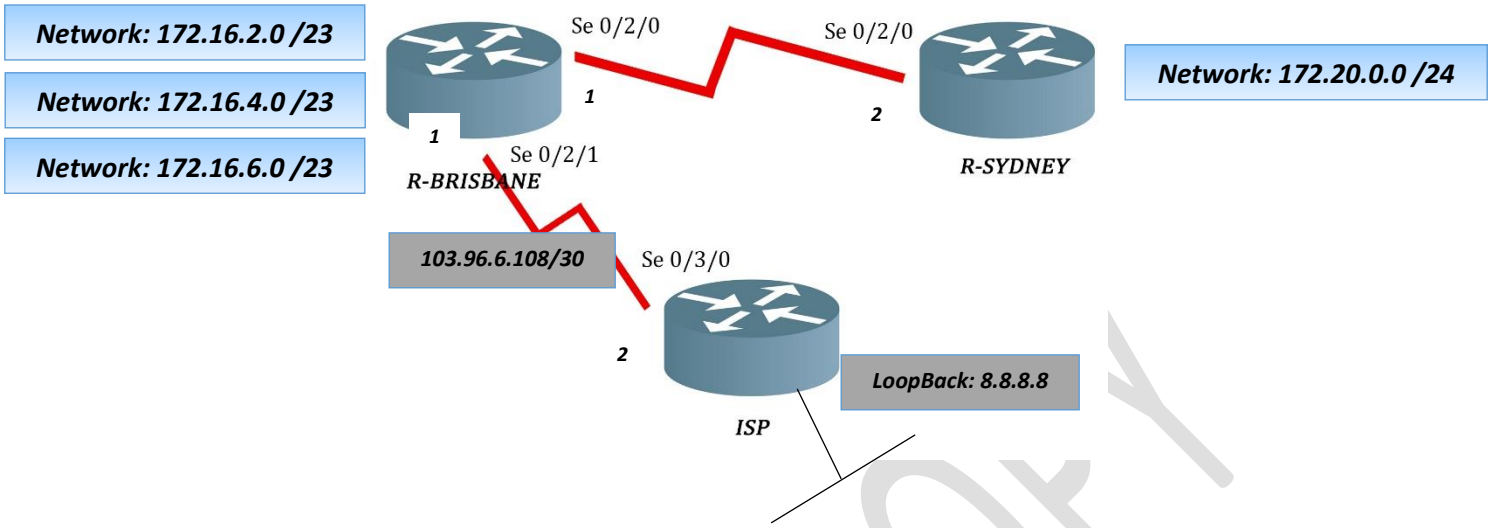
The Western Mining company has informed us that the communication and connection between both offices will be standardized under the ospf (Open Shortest Path First) protocol as well as the link that will allow both networks to have full access to the internet.

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:

172.16.8.0/30

Network: 172.16.0.0 /23



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	0.0.1.255	Fa 0/0.20
			Network 172.16.2.0	0.0.1.255	Fa 0/0.30
			Network 172.16.4.0	0.0.1.255	Fa 0/0.40
			Network 172.16.6.0	0.0.1.255	Fa 0/0.50
			Network 172.16.8.0	0.0.0.3	
			Network 103.96.6.108	0.0.0.3	
1	0	R-SYDNEY	Network 172.20.0.0	0.0.0.255	Fa 0/0
			Network 172.16.8.0	0.0.0.3	
1	0	ISP	Network 103.96.6.108	0.0.0.3	
			Network 8.8.8.8	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 m

st 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*

(TASK 3) Fully Costed Bill:

Provided to:
Western Mining

Attention: Jack Crusher, Branch Office Manager, Western Mining

Quantity	Item	Model	Function	Cost	Vendor
192 (48 per Department)	Pc-Computers	Dell Optiplex 9010 SFF	Main communication device for staff	$ 48,888 AUD $ 239 /Each	Australian Computer Traders
192 (48 per Department)	Monitors	Philips 223V5LHSB2 21.5 " VGA HDMI	Cpu display interface	$ 22,080 AUD $115 /Eeach	Centrecom
192 (48 per Department)	Mouse and Keyboards	Rapoo x120 pro wired optical mouse and keyboard combo	CPU control interfaces	$ 2304 AUD $ 12 /Each	Centrecom
196 (49 per Department)+1 (Mainswitch – Router)	Cable	10 M. RJ45 CAT6 Ethernet Cable	Cables connecting hosts and servers to the switch´s department.10 meters.	$ 4,304 AUD $ 21,85 /Each	4 Cabling
8	Cable	3 M. CAT 5E RJ45-RJ45 Crossover Cable	Cables connecting between switches	$ 80.72 AUD $ 10.09 /Each	4 Cabling
9	Switches	Cisco Catalyst 2960 24 10/100 +2 1000bt Lan Base Image ws-c2960-24-TT-L-RF	Switches in charge of gathering and connecting the traffic through the network.	$ 8,750.88 AUD $ 972.32/Each	The Telecomshop
1	Router	Cisco 2811 Integrated Services Router	In charge of routing traffic to other networks	$ 1071 AUD	U-buy
1	The Cisco Gigabit Ethernet High-Speed WAN Interface Card (HWIC)	HWIC-1GE-SFP	Connector to have the possibility of having a gigabit interface in the event of needing a high-speed port	$ 316 AUD	4startech

1	Cisco High-Speed Wan Interface Card	HWIC-2T	Possibility to have two serial interfaces that will be essential for wan routing.	$ 218	4startech
			Total	**88, 011.72**	

On acceptance of quotation terms and conditions please sign and return to office with a purchase order so that work may commence.

Item	Model	
Pc-Computers	Dell Optiplex 9010 SFF	
Monitors	Philips 223V5LHSB2 21.5 " VGA HDMI	
Mouse and Keyboards	Rapoo x120 pro wired optical mouse and keyboard combo	
Cable	10 M. RJ45 CAT6 Ethernet Cable	
Cable	3 M. CAT 5E RJ45-RJ45 Crossover Cable	

Switches	Cisco Catalyst 2960 24 10/100 +2 1000bt Lan Base Image ws-c2960-24-TT-L-RF	
Router	Cisco 2811 Integrated Services Router	
The Cisco Gigabit Ethernet High-Speed WAN Interface Card (HWIC)	HWIC-1GE-SFP	
Cisco High-Speed Wan Interface Card	HWIC-2T	

- ***Excel spreadsheet with bill of materials with individual and total cost, Attached in sending files.***

(TASK 4) IP Address sheme:

Configuration

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

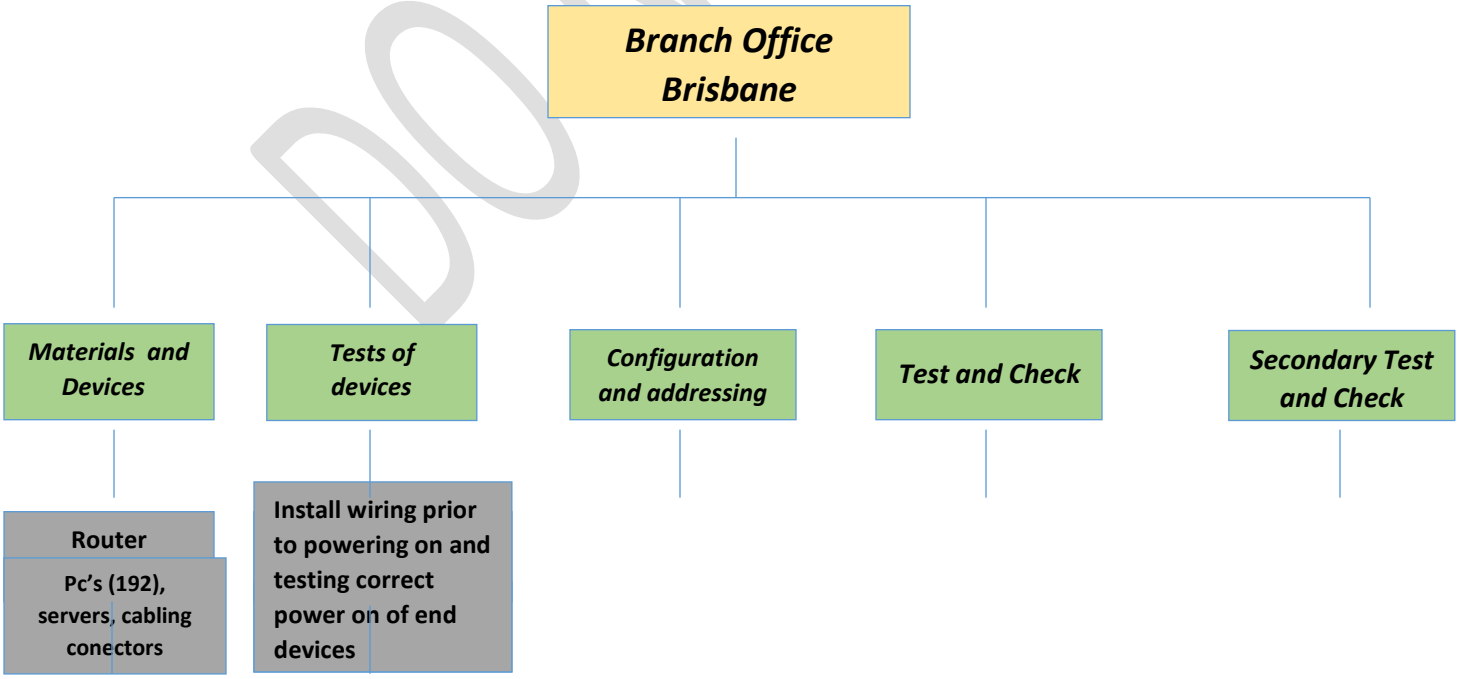
Sales	510	512	172.16.0.0 /23	172.16.0.1	172.16.1.254	172.16.1.255	255.255.254.0
Operations	510	512	172.16.2.0 /23	172.16.2.1	172.16.3.254	172.16.3.255	255.255.254.0
Managements	510	512	172.16.4.0 /23	172.16.4.1	172.16.5.254	172.16.5.255	255.255.254.0
Exploration	510	512	172.16.6.0 /23	172.16.6.1	172.16.7.254	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

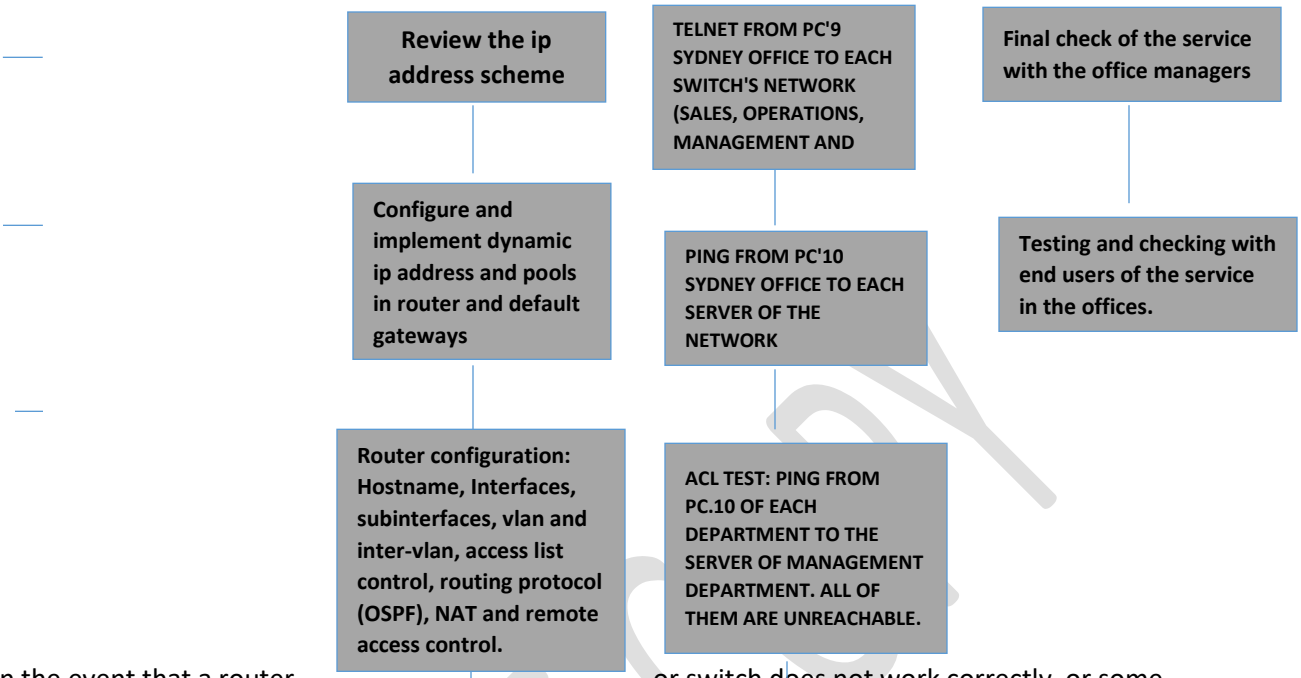
Clearly this scheme will satisfy the amount of staff required by department in addition to giving us an IP range for the addresses between both offices.

_Why is important to document this kind of network information?

First of all, having and documenting this type of information will allow us to configure each device correctly. In other words, it will allow us to subdivide the networks by department giving us the opportunity to assign an IP address to each device that requires it, so in this way we can configure security protocols, internet connection and differentiate each equipment and solve any problem that may arise individually.

(TASK 5) Work Breakdown for the network installation.





In the event that a router or switch does not work correctly, or some contingency happens, we could recommend the following equipment in its replacement.

Routers: Cisco Router 1941, Cisco Router 2901

Switches: Cisco Switch Pt-Switch 2950- 24, Cisco Empty, Cisco Switch 2950t.

(TASK 6) Potential safety hazards and recommended precautions.

Router 2811:

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

Statement 1—Power Disconnection Warning

Warning: Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.

Power Supply Warning

Warning: Do not touch the power supply when the power cord is connected. For systems with a power switch,

line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.

TN Power Warning

Warning: The device is designed to work with TN power systems.

ISDN Connection Warning

Warning: The ISDN connection is regarded as a source of voltage that should be inaccessible to user contact. Do not attempt to tamper with or open any public telephone operator (PTO)-provided equipment or connection hardware. Any hardwired connection (other than by a nonremovable, connect-one-time-only plug) must be made only by PTO staff or suitably trained engineers.

Ground Connection Warning

Warning: When installing the unit, always make the ground connection first and disconnect it last.

Jewelry Removal Warning

Warning: Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Lifting the Chassis Warning

Warning: Two people are required to lift the chassis. Grasp the chassis underneath the lower edge and lift with both hands. To prevent injury, keep your back straight and lift with your legs, not your back. To prevent damage to the chassis and components, never attempt to lift the chassis with the handles on the power supplies or on the interface processors, or by the plastic panels on the front of the chassis. These handles were not designed to support the weight of the chassis.

Hazardous Network Voltages Warning

Warning: Hazardous network voltages are present in the BRI S/T, BRI U, CT1/PRI-CSU, CE1/PRI-B, CE1/PRI-U ports regardless of whether power to the router is OFF or ON. To avoid electric shock, use caution when working near these ports. When detaching cables, detach the end away from the router first.

WAN Interface Card Insertion Warning

Warning: To avoid electric shock, do not insert a WAN interface card into a 2-slot module while power to the router is ON or network cables are connected.

Wrist Strap Warning

Warning: During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Circuit Breaker (15A) Warning

Daniel Cortez Assessment Install Network

Warning: This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a UL Listed and Certified fuse or circuit breaker no larger than 60 VDC, 15 A is used on all current-carrying conductors.

Safety Cover Requirement

Warning: The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.

Exposed DC Power Wire Warning

Warning: An exposed wire lead from a DC-input power source can conduct harmful levels of electricity. Be sure that no exposed portion of the DC-input power source wire extends from the terminal block plug.

Power Off Before Working on System

Warning: Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.

T1/E1 Connection Warning

Warning: The T1/E1 connection is regarded as a source of voltage that should be inaccessible to user contact. Do not attempt to tamper with or open any public telephone operator (PTO)-provided equipment or connection hardware. Any hardwired connection (other than by a nonremovable, connect-one-time-only plug) must be made only by PTO staff or suitably trained engineers.

Grounding Requirement Warning

Warning: This equipment needs to be grounded. Use a green and yellow 14 AWG ground wire to connect the host to earth ground during normal use.

DC Power Supply Warning

Warning: The illustration shows the DC power supply terminal block. Wire the DC power supply using the appropriate lugs at the wiring end, or with no lugs, as illustrated. The proper wiring sequence is ground to ground, positive to positive, and negative to negative. Note that the ground wire should always be connected first and disconnected last.

DC Power Supply Wiring Warning

Warning: The illustration shows the DC power supply terminal block. Wire the DC power supply as illustrated. The proper wiring sequence is ground to ground, positive to positive, and negative to negative. The ground wire should always be connected first and disconnected last.

Unit Mounting Warning

Warning: This unit is intended to be mounted on a wall. Please read the wall mounting instructions carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system.

AC Power Grounding Warning

Daniel Cortez Assessment Install Network

Daniel Cortez Assessment Install Network

Warning: AC connected units must have a permanent ground connection in addition to the power cable ground wire. NEBS-compliant grounding satisfies this requirement.

Work During Lightning Activity

Warning: Do not work on the system or connect or disconnect cables during periods of lightning activity.

DC Power Supply

Warning: When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These terminations should be the appropriate size for the wires and should clamp both the insulation and conductor.

DC Power Disconnection

Warning: Before performing any of the following procedures, ensure that power is removed from the DC circuit.

Installation Instructions

Warning: Read the installation instructions before connecting the system to the power source.

Circuit Breaker

Warning: This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:
60 VDC, 30 A

Circuit Breaker

Warning: This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:
120 VAC, 15 A U.S. (240 VAC, 10A international)

Chassis Warning for Rack-Mounting and Servicing

Warning: To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

• This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
• When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
• If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

TN and IT Power Systems

Warning: This equipment has been designed for connection to TN and IT power systems.

Class 1 Laser Product

Daniel Cortez Assessment Install Network

Daniel Cortez Assessment Install Network

Warning: Class 1 laser product.

Battery Handling Warning

Warning: There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Restricted Area

Warning: This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.

Main Disconnecting Device

Warning: The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.

SELV Circuit

Warning: To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

Ground Conductor

Warning: This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Use Copper Conductors Only

Warning: Use copper conductors only.

WAN Port Static Shock

Warning: Hazardous network voltages are present in WAN ports regardless of whether power to the router is OFF or ON. To avoid electric shock, use caution when working near WAN ports. When detaching cables, detach the end away from the router first.

More Than One Power Supply

Warning: This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.

Blank Faceplates and Cover Panels

Warning: Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.

Equipment Installation

Daniel Cortez Assessment Install Network

Daniel Cortez Assessment Install Network

Warning: Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Lifting the Chassis

Warning: To prevent personal injury or damage to the chassis, never attempt to lift or tilt the chassis using the handles on modules (such as power supplies, fans, or cards); these types of handles are not designed to support the weight of the unit.

Telephone Jacks in Wet Locations

Warning: Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.

Uninsulated Wires or Terminals

Warning: Never touch uninsulated telephone wires or terminals unless the telephone line has beendisconnected at the network interface.

Product Disposal

Warning: Ultimate disposal of this product should be handled according to all national laws and regulations.

Disconnecting Telephone-Network Cables

Warning: Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.

Installation Hazard

Warning: This equipment must be installed and maintained by service personnel as defined by AS/NZS 3260. Incorrectly connecting this equipment to a general-purpose outlet could be hazardous. The telecommunications lines must be disconnected 1) before unplugging the main power connector or 2) while the housing is open, or both.

Short-circuit Protection

Warning: This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

Installing or Replacing the Unit

Warning: When installing or replacing the unit, the ground connection must always be made first and disconnected last**.**

Overheating Prevention

Warning: To prevent the system from overheating, do not operate it in an area that exceeds the maximumrecommended ambient temperature of: 40°C (104°F)

Remove Power Before Disconnecting

Warning: Do not disconnect connections to this equipment unless power has been removed or you have verified that the area is nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. Substitution of components may impair suitability for Class I, Division 2.

Daniel Cortez Assessment Install Network

Daniel Cortez Assessment Install Network

Do Not Operate Unit Without Covers

Warning: The covers are an integral part of the safety design of the product. Do not operate the unit without the covers installed

Switch 2690:

This section includes the basic installation warning statements. Translations of these warning statements appear in the *Regulatory Compliance and Safety Information for the Catalyst 2960 Switch* guide.

Warning Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

Warning To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 113°F (45°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.

Warning Installation of the equipment must comply with local and national electrical codes.

Warning To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety: This unit should be mounted at the bottom of the rack if it is the only unit in the rack.When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Warning This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Warning If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch.

Warning Class 1 laser product.

Warning For connections outside the building where the equipment is installed, the following ports must be connected through an approved network termination unit with integral circuit protection: 10/100/1000 Ethernet.

Warning Voltages that present a shock hazard may exist on Power over Ethernet (PoE) circuits if interconnections are made using uninsulated exposed metal contacts, conductors, or terminals. Avoid using such interconnection methods, unless the exposed metal parts are located within a restricted access location and users and service people who are authorized within the restricted access location are made aware of the hazard. A restricted access area can be accessed only through the use of a special tool, lock and key or other means of security.

(TASK 7) **The power and data quote provided and draft response to the branch office manager.**

ELECTRICAL AND DATA QUOTE

Provided to:
Attention: Jack Crusher, Branch Office Manager, Western Mining

Daniel Cortez Assessment Install Network

Daniel Cortez Assessment Install Network

We reviewed the electrical and data quote and all items appear to be according to the design proposed by Pacific It Solutions.

We proceed to approve the shopping list and agree on the arrival of these.

If you have any questions, do not hesitate to contact us.

Have a nice day.

Daniel Cortez Network Engineer
Pacific IT Solutions
QLD, Australia

(TASK 8) **Email for your network design submission to the appropriate person.**

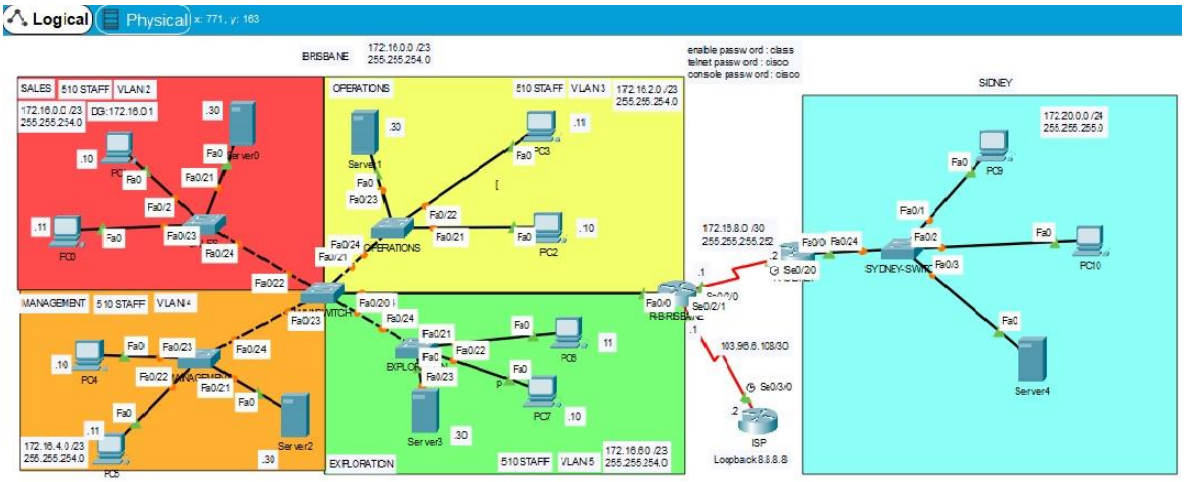
Provided to:

Daniel Cortez Assessment Install Network

Daniel Cortez Assessment Install Network

Western Mining
Attention: Deana Troy, Senior Systems Architect, Western Mining

According to what was previously discussed, I proceed to send the final design of the network proposed by Pacific IT Solutions, in the format of the packet tracer program where the functions, tests, designs, implements, tools and the different devices can be viewed and checked efficiently to be implemented.



Of course, any questions, comments or requirements do not hesitate to let us know.

In addition to the design in packet tracer format, I attach the following files: Network Description, fully costed bill and network diagram (work breakdown).

Thank you for choosing Pacific IT Solutions for your network design.

Daniel Cortez Network Engineer
Pacific IT Solutions
QLD, Australia

Daniel Cortez Assessment Install Network

(TASK 9) Email to the branch office manager to coordinate the network installation.

Provided to:

Western Mining

Attention: Jack Crusher, Branch Office Manager, Western Mining

According to the response of the sent design, this was duly reviewed and its approval was reached, therefore I sent this email to coordinate the installation of the network and its devices on the date that we could jointly agree on the date that is estimated convenient. We recommend agreeing on a suitable date in order to coordinate the purchase of materials, create a schedule for our staff and be able to properly test the components.

I take this opportunity to request access to the installation site of the network on the date where the process is agreed.

It would also be of great help to obtain the design and electrical diagram to create the safety plan.

Of course, our offices and I personally will be ready for any request or query that may arise.

Thank you for choosing Pacific IT Solutions for your network design.

Daniel Cortez Network Engineer
Pacific IT Solutions
Qld, Australia

(TASK 10) Packet Tracer:

- ***Network using Packet Tracer, attached in sending files.***

(TASK 11) Table with a list of the network functionality requirements and the validation checks and diagnostic tests:

- ***List of test, attached in sending files.***

(TASK 12) Email to the branch office manager requesting sign off for the completed network installation.

Provided to:
Western Mining

Attention: Jack Crusher, Branch Office Manager, Western Mining

I send this email after having received all the previously approved proposals: design, service, security and implementation proposal for the new Brisbane office network and thus request final approval for the process.

I also take the opportunity to recommend the nbn service again. Our team is ready for the configuration and implementation.

Telnet passwords for all devices is cisco and also the connectivity results are attached task 11 list of test.

Without further ado, I await your response and we will continue to listen to any requirement.

Have a great day.

(TASK 13) NBN has been rolled out.

Provided to:
Western Mining

Attention: Deana Troy, Senior System Architect, Western Mining

As we have already found out, the company nbn has been installed and will be available for the implementation of the internet service for the area where the office is located. According to what has been discussed and previously requested, since it is necessary to change the provider, I recommend evaluating the possibility of using the Nbn service since it will give you the opportunity to make the service faster and cheaper with a download capacity of up to 100 mbps.

This is because of using fibre optic as the media.

The price will also be much more convenient since this service will only cost $ 99.99 per month, while other companies could cost between $ 1500 and $ 3000 dollars per month. Although it is true that this service can be more secure because the wan link is private and specific to the office while nbn is public, this could be solved by creating a connection tunnel between the office and the provider with the "VPN" method. So this would be solved quickly and efficiently.

If you have any questions, do not hesitate to contact me so we can arrange a meeting to resolve the problem.

Have an excellent day

Daniel Cortez Assessment Install Network

Daniel Cortez Network Engineer
Pacific IT Solutions
Qld, Australia

(TASK 14)

- ***Network using Packet Tracer, attached in sending files.***

(TASK 15) Conduct a wireless site survey:

When conducting a wireless site survey, consider the following steps and tips:

1. Understand the wireless requirements. In order to identify optimum locations for access points or mesh nodes, you must have a good understanding of specific requirements for the network that impacts signal coverage. For example, maximum range between a client device and the access point decreases as data rate and resulting performance increases. Thus, you need to know the target data rates (and throughput) to correctly interpret survey results. Also, client devices may have relatively low transmit power, which must be taken into consideration when using most site survey tools.

2. Obtain a facility diagram. Before getting too far with the site survey, locate a set of building blueprints or city maps. If none are available, prepare a drawing that depicts the location of walls, walkways, etc. Site survey tools import diagrams in various image formats. Of course mapping software is a good source for outdoor city surveys. If all else fails for inbuilding surveys, consider taking a digital photograph of the fire escape diagram, which is usually present on hallway walls.

3. Visually inspect the facility. Walk through the facility before performing any testing to verify the accuracy of the facility diagram. This is a good time to note any potential attenuation barriers that may affect the propagation of RF signals. For example, a visual inspection will uncover obstacles to signals such as metal racks and partitions, items that blueprints generally don't show. Also, note possible locations for mounting access points, such as above ceiling tiles or on pillars. For outdoor city environments, you should carefully assess the locations and availability of street lights and water towers for mounting mesh nodes and backhaul equipment. These actions will make the later testing efforts go much more smoothly.

4. Assess existing network infrastructure. Determine the capacity of any existing wired networks that can interface the access points or mesh nodes. Most buildings have Ethernet and in some cases optical fiber networks. Check on how much of the existing networks can be made available for supporting the wireless network. This will aid designers later on in the deployment when defining the architecture and bill of materials for the wireless network.

5. Identify coverage areas. On the facility diagram or city map, indicate all areas where coverage is needed, such as offices, hallways, stairwells, utility rooms, bathrooms, break rooms, patios, parking garages, and elevators. Also, identifying where users will not wireless coverage is important to avoid wasting time surveying unnecessary areas. Keep in mind that you might get by with fewer access points and lower equipment costs if you can limit the roaming areas.

Daniel Cortez Assessment Install Network

6. Determine preliminary access point locations. By considering the location of wireless users and range estimations of the wireless LAN products you're using, approximate the locations of access points that will provide adequate coverage throughout the user areas. Plan for some propagation overlap (generally 25 percent) among adjacent access points, but bear in mind that channel assignments for access points will need to be far enough apart to avoid interaccess point interference.

Be certain to consider mounting locations, which could be vertical posts or metal supports above ceiling tiles. Recognize suitable locations for installing the access point, antenna, and data / PoE cable. Also think about different antennas when deciding where to position access points. An access point mounted near an outside wall, for example, could be a good location if you use a patch antenna with relatively high gain oriented within the facility.

7. Verify access point locations. This is when the site survey testing begins. Most wireless LAN vendors provide wireless site survey software that identifies the associated access point, data rate, signal strength, and signal quality. You can load this software on a laptop and test the coverage of each preliminary access point location. Alternately, you can use a third party site survey tool available from several different companies, such as AirMagnet, Berkeley Varitronics Systems, and Ekahau.

Install an access point at each preliminary location, and monitor the site survey tool readings by walking varying distances away from the access point. There's no need to connect the access point to the distribution system because the survey tests merely ping the access point or read the beacon signal strength. Very important: Definitely consider the SNR range boundary and uplink signal strength when interpreting the results. To make the access point easy to move about the facility, you can mount it on a pole attached to a cart with a battery and DC/AC converter. Otherwise, you'll need to haul around an extension cord and always be looking for where to plug in for power (not recommended).

Take note of performance or signal readings at different points as you move to the outer bounds of the access point coverage. In a multifloor facility, perform tests on the floor above and below the access point. Keep in mind that a poor signal quality reading could indicate that RF interference is affecting the wireless LAN. This would warrant the use of a spectrum analyzer to characterize the interference, especially if there are no other indications of its source. Based on the results of the testing, you might need to reconsider the location of some access points and redo testing for the affected locations.

8. Document findings. Once you're satisfied that the location of access points you've identified will provide adequate signal coverage, document your findings on the facility diagrams by depicting the location of each access point. The installers will need this information.

These steps will point you in the right direction, but experience really pays off. If you're new to wireless LANs, you'll begin to build an odd intuition about the propagation of radio waves after accomplishing several wireless site surveys.