CAPÍTULO V

IMPLANTACIÓN

5.1- Introducción

Este capítulo puntualiza el proceso en efecto que se acogerá para la realización de la reingeniería de la red IP de PETROCOMERCIAL Quito y la optimización de su seguridad perimetral, detallando por lo tanto las actividades que impliquen la implementación e implantación de dicho proyecto. Es fundamental para esto presentar las configuraciones de los equipos utilizados, aquí se incluyen switches “Cisco”, la central telefónica IP “Mitel” y el equipo de seguridad perimetral “Astaro”.

Para ejecutar las configuraciones incluidas en este capítulo se realizaron inicialmente pruebas a modo de laboratorio, mediante equipos disponibles y fuera de producción que posee la empresa. Dichos equipos de prueba poseen las mismas características de los equipos que se utilizaran en el proyecto, brindando la posibilidad de reforzar el proceso de instalación y configuración de los equipos.

En relación a la configuración de los equipos de conmutación, se debe indicar que las configuraciones serán realizadas a través de sus interfaces de línea de comandos (CLI), puesto que este modo de configuración presta

capacidades superiores de control, mientras la central telefónica IP y el equipo de seguridad perimetral, los cuales poseen un sistema operativo basado en UNIX, serán configurados a través de sus interfaces Web, gráficas e intuitivas, que permiten la configuración completa de los equipos.

5.2- Configuraciones

Todas configuraciones requeridas para la realización del presente proyecto se especificarán a continuación a nivel de dispositivos, siendo estos los switches CISCO, la central telefónica IP MITEL, el servidor DHCP, y el equipo de seguridad perimetral ASTARO.

5.2.1- Switches CISCO

Previo a la configuración básica de los equipos de conmutación es esencial identificar las particularidades de los sistemas operativos de los mismos. En el siguiente cuadro se indican las principales características de todas las versiones de switches Cisco Catalyst que se utilizarán para la reingeniería de la red IP.

Cuadro 5.1 : Características técnicas de los Switches Cisco Catalyst

Característica \ SWITCH	Catalyst 2924	Catalyst 3524	Catalyst 3560	Catalyst 4507 (Supervisor Engine IV
Version del software (IOS)	12.0(5.2)XU	12.0(5)WC3b	12.2(25)SEE2	12.2(18)EW3
Gigabit Ethernet		X	X	X
Fast Ethernet	X	X	X	X
IEEE 802.1D STP	X	X	X	X
IEEE 802.1w Rapid STP			X	X
Número de instancias STP	64	64	128	3000
IEEE 802.1p CoS	X	X	X	X
IEEE 802.1Q / ISL	X	X	X	X
VTP version 1	X	X	X	X
VTP version 2	X	X	X	X
Número máximo de VLANs	68	254	1005	1005
Throughput (Tasa de transferencia)	3Mpps	6.5Mpps	13.1 Mpps	48Mpps
Capa 2	X	X	X	X
Capa 3			X	X
PoE		X	X	X
Cisco Works	X	X	X	X
Clustering	X	X	X	
Port ACLs	X	X	X	X
VLAN ACLs (Access Maps)			X	X

Conjuntamente es preciso aclarar el especial funcionamiento de algunas de las características mencionadas, como son:

- ✓ Las VLAN IDs desde 1002 hasta 1005 son reservadas para VLANs Token Ring y FDDI.
- ✓ El protocolo VTP aprende únicamente el rango estándar de VLANS es decir desde 1 hasta el máximo número de VLANs, dependiendo del equipo.
- ✓ Los VLAN IDs mayores a 1005 son VLANs de rango extendido y no se almacenan en la base de datos de las VLANs.
- ✓ Un enlace troncal entre switches soporta 1005 VLANs, el protocolo de encapsulación ISL soporta 1000 VLANs y el protocolo de encapsulación 802.1Q soporta 4096 VLANs.

5.2.1.1- Configuración básica de switches

Existen dos modos de comandos para un switch Cisco. El modo por defecto es el modo EXEC usuario (ejecución a modo usuario) , este se lo reconoce por su indicador, que termina en un carácter de "mayor que" (**>**). Los comandos disponibles en el modo EXEC usuario se limitan a quienes realizan cambios a las configuraciones de terminal, realizan pruebas básicas y muestran información del sistema.

El comando enable se utiliza para entrar al modo EXEC privilegiado (ejecución a modo privilegiado) desde el modo EXEC usuario, a este se lo reconoce por su indicador, que termina con el carácter numeral (#). El conjunto de comandos del modo EXEC privilegiado incluye el comando configure así como todos los comandos del modo EXEC usuario. El comando **configure** permite el acceso a otros modos de comando. Dado que estos modos se utilizan para configurar el switch, el acceso al modo EXEC privilegiado debe protegerse con contraseña para evitar el uso no autorizado. Es entonces fundamental como paso inicial determinar los datos y las contraseñas de los equipos. En todos los switches Cisco Catalyst se debe configurar lo indicado en el siguiente cuadro:

Cuadro 5.2 : Pasos para la configuración básica de los switches Cisco.

Parámetro a configurar	Comandos
Contraseña EXEC usuario	enable password *clave*
Contraseña EXEC privilegiado	enable secret *clave*
Encriptación de claves	service password-encryption
Nombre del equipo	hostname *nombre*
Mensaje de descripción del equipo	banner motd *mensaje*
Contraseña consola	line con 0
	Password *clave*

	Login
	line vty 0 15 / line vty 0 4 / line vty 5 15
	password *clave*
Contraseña para accesos telnet	Login
Habilitar el uso de la subred 0	Ip subnet-zero

Se debe notar que todos los comandos para la configuración básica son accesados desde el modo de configuración EXEC privilegiado, y luego ingresando al modo de configuración global mediante el comando *configure terminal*.

A continuación se muestra la configuración básica de uno de los switches de PETROCOMERCIAL Quito, aplicando la información correspondiente al equipo, tomando en cuenta que las claves de acceso ya se encuentran encriptadas.

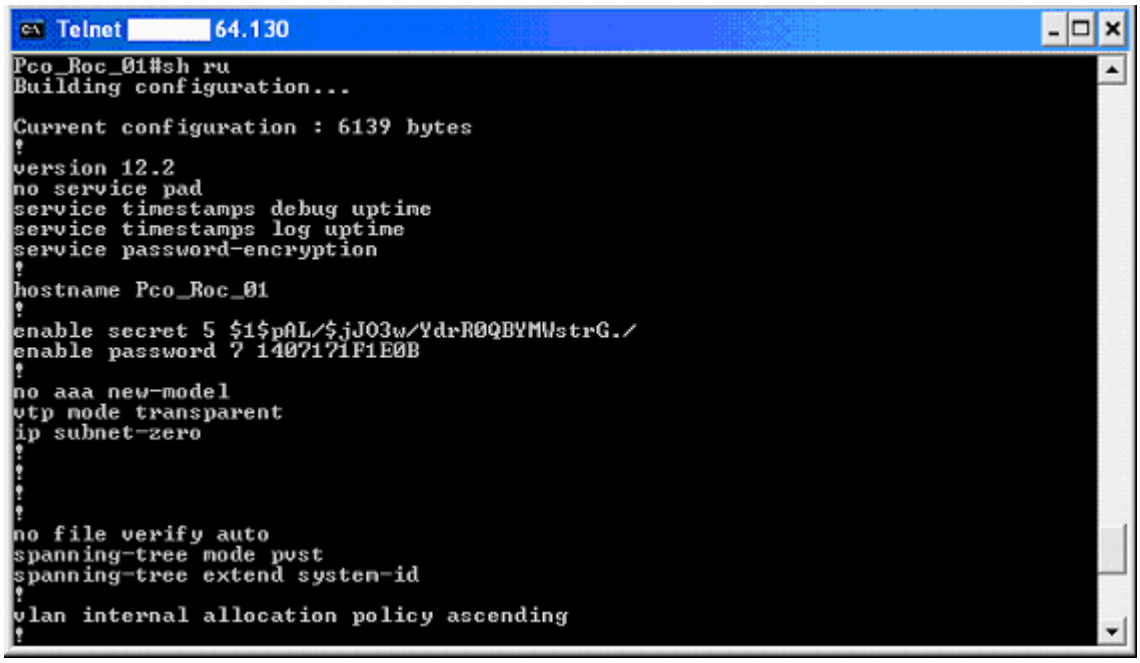


Figura 5.1: Pantalla de configuración básica Switch Pco_Roc_01

Conjuntamente se describe la configuración completa del equipo:

Switch PCO-PlantaBaja

User Access Verification

Password:

Pco_Roc_01>en

Password:

Pco_Roc_01#sh ru

Building configuration...

Current configuration: 6139 bytes

version 12.2

no service pad

service timestamps debug uptime

service timestamps log uptime

service password-encryption

hostname Pco_Roc_01

enable secret 5 1pAL/$jJO3w/YdrR0QBYMWstrG./

enable password 7 1407171F1E0B

no aaa new-model

vtp mode transparent

ip subnet-zero

no file verify auto

spanning-tree mode pvst

spanning-tree extend system-id

banner motd ^CSwitch PCO-PlantaBaja^C

line con 0

password 7 11191C11051D

login

line vty 0 4

password 7 06160A355E41

login

line vty 5 15

no login

end

Es importante mencionar que en los equipos Cisco, el archivo *running-config*, es el archivo de configuración activo del switch el cual se almacena en la memoria volátil del equipo (RAM), y el archivo *startup-config* contiene la última configuración que haya sido guardada en la memoria no volátil del equipo (NVRAM), por lo que para almacenar la configuración del equipo luego de realizar algún cambio, es necesario copiar el archivo *running-config,* en el archivo *startup-config*, para esto se ingresa desde el modo EXEC privilegiado el comando ***copy running-config startup-config***, luego de que hayan sido ejecutados los cambios respectivos a las configuraciones de los equipos.

5.2.1.2- Configuración de VLANs y asignación por puertos

Como se explicó en el capítulo anterior se designarán VLANs por puertos. Para ello se asignará a cada puerto la VLAN que corresponda de acuerdo al grupo al que pertenezca el equipo que esta conectado a ese puerto.

Previo a la asignación de puertos, en el switch de core, en este caso el Cisco Catalyst 4500, se debe realizar la configuración de las VLANs que se crearán, puesto que posteriormente están serán propagadas al resto de switches de la red de PETROCOMERCIAL Quito, a través del protocolo VTP. Para acceder a la configuración de VLANs se debe ingresar al modo de administración con privilegios y digitar los comandos respectivos.

Para crear una de las VLANs requeridas se debe configurar lo siguiente:

Cuadro 5.3 : Pasos para la creación de VLANs en los switches Cisco

Parámetro a configurar	Comando
Ingresar al modo configuración de VLANs	vlan database
Añadir una VLAN	vlan *vlan-id* name *nombre_vlan*
Guardar los cambios	apply
Verificar la VLAN creada	show vlan
Asignar dirección IP a la VLAN	configure terminal
	interface *vlan-id*
	ip address *puerta de enlace-VLAN máscara de subred-VLAN*
	no shut
Verificar toda la configuración de la VLAN	show running-config

Para borrar una VLAN desde el modo de configuración de VLANs se ingresa el comando **no vlan *vlan-id*.**

A continuación se muestra la configuración de VLANs creadas en el switch de core de PETROCOMERCIAL Quito, Cisco Catalyst 4500, aplicando la información correspondiente a este equipo:

Figura 5.2: Pantalla de configuración de VLANs en el Switch Pco_Roc_P50

Conjuntamente se describe la configuración completa del equipo:

interface Vlan1

description VLAN GENERAL

ip address X.Y.69.1 255.255.255.0

ip helper-address X.Y.64.21 255.255.255.128

!

interface Vlan10

description VLAN EQUIPOS EMPRESARIALES

ip address X.Y.64.1 255.255.255.128

!

interface Vlan20

description VLAN ADMINISTRACION DE EQUIPOS

ip address X.Y.64.129 255.255.255.192

!

interface Vlan30

description VLAN USUARIOS ESPÈCIALES

ip address X.Y.64.193 255.255.255.192

!

interface Vlan40

description VLAN USUARIOS DE SISTEMAS

ip address X.Y.65.1 255.255.255.128

ip helper-address X.Y.64.21 255.255.255.128

!

interface Vlan50

description VLAN INDUSTRIAL

ip address X.Y.65.129 255.255.255.128

ip helper-address X.Y.64.21 255.255.255.128

!

interface Vlan60

description VLAN ADMINISTRATIVA

ip address X.Y.66.1 255.255.254.0

ip helper-address X.Y.64.21 255.255.255.128

!

interface Vlan70

description VLAN COMERCIALIZACIÓN

ip address X.Y.68.1 255.255.255.0

ip helper-address X.Y.64.21 255.255.255.128

!

interface Vlan1001

description VLAN VOIP

ip address X.Y.70.1 255.255.254.0

!

Nota: El comando ***ip helper-address*** que se muestra en la configuración indicada recientemente, se explicará posteriormente en la configuración del servidor DHCP.

Ya definidas las VLANs, se puede asignar a los puertos la VLAN a la que concernirán. Esta asignación se la debe hacer escrupulosamente puesto que dependerá del equipo conectado hacia cada puerto. Existen tres escenarios que se presentan al momento de asignar un puerto a una VLAN, independientemente de la VLAN a la que correspondan, puesto que el puerto puede estar conectado a:

- ✓ Una PC

- ✓ Un equipo (servidores y/o equipos afines)
- ✓ Un teléfono IP
- ✓ Una PC y un teléfono IP

Para que los puertos conectados a una PC u otros equipos sean asignados a la VLAN a la cual pertenecen, se debe configurar lo indicado en el siguiente cuadro:

Cuadro 5.4 : Pasos para la asignación de interfaces a VLANs en los switches Cisco.

Parámetro a configurar	Comando
Ingresar al modo de configuración	configure terminal
Ingresar a un puerto del switch	interface fastEthernet *puerto-id* **/** gigabitEthernet *puerto-id*
Definir el modo de membresia	switchport mode access
Agregar el puerto a una VLAN	switchport access vlan *vlan-id*
Salir de la configuración	end
Verificar el puerto configurado	show running-config

En el caso de asignarse una interfaz a una VLAN que no haya sido creada, una nueva VLAN se creará.

Para que los puertos conectados exclusivamente a un teléfono IP sean asignados a la VLAN a la cual pertenecen (VLAN 1001 VOIP), se debe configurar lo indicado en el siguiente cuadro:

Cuadro 5.5 : Pasos para la asignación de interfaces a la VLAN de voz en los switches Cisco.

Parámetro a configurar	Comando
Ingresar al modo de configuración	configure terminal
Ingresar a un puerto del switch	interface fastEthernet *puerto-id* **/** gigabitEthernet *puerto-id*
Agregar el puerto a la VLAN de Voz	switchport voice vlan **1001**
Salir de la configuración	end
Verificar el puerto configurado	show running-config

En el caso de los puertos conectados a un teléfono IP y que a través de este se conectan a una PC, su configuración consiste en los siguientes pasos:

Cuadro 5.6 : Pasos para la asignación de interfaces a VLAN de voz y datos en los switches Cisco.

Parámetro a configurar	Comando
Ingresar al modo de configuración	configure terminal
Ingresar a un puerto del switch	interface fastEthernet *puerto-id* **/** gigabitEthernet *puerto-id*
Definir el modo de membresia	switchport mode access
Agregar el puerto a una VLAN	switchport access vlan *vlan-id*
Agregar el puerto a la VLAN de Voz	switchport voice vlan **1001**
Salir de la configuración	end
Verificar el puerto configurado	show running-config

Es substancial indicar que los comandos indicados son utilizados a partir de la versión 12.2 de I.O.S. de los equipos Cisco, para el caso de los switches Cisco Catalyst 2924 y 3524, los cuales poseen versiones anteriores de I.O.S., cabe señalar que los cambios a las configuraciones ya indicadas son mínimos Por citar un ejemplo, la asignación de puertos para los tres casos seria de la siguiente manera:

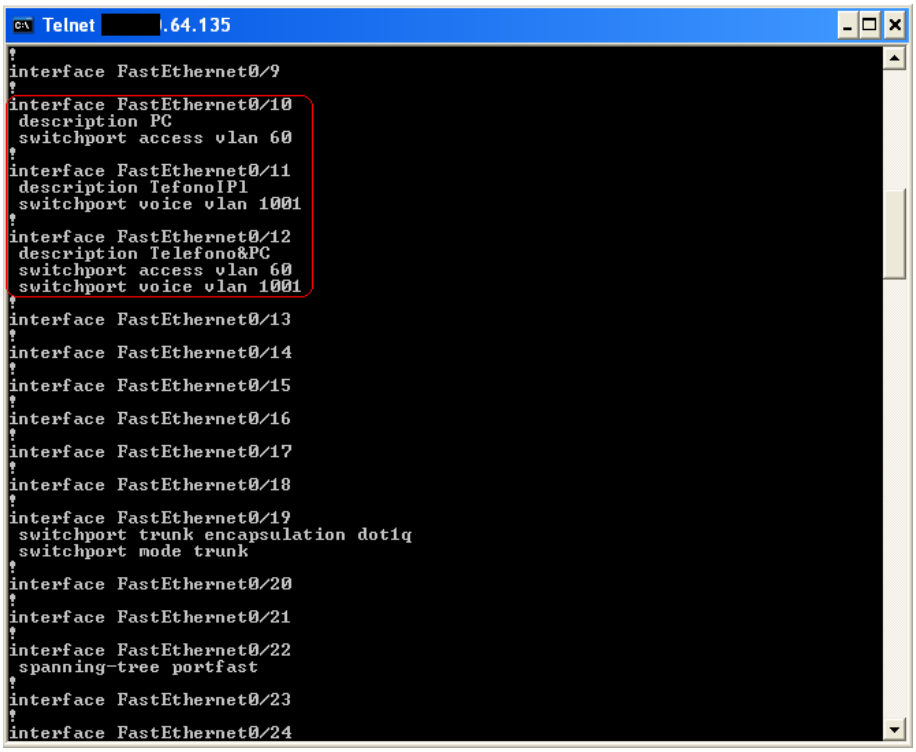


Figura 5.3: Pantalla de configuración de puertos en el Switch Pco_Roc_P10

Conjuntamente se describe la configuración completa del equipo:

```
 interface FastEthernet0/1
 description PC
 switchport access vlan 60
 switchport mode access
 no ip address
!
interface FastEthernet0/2
description TeléfonoIP
switchport voice vlan 1001
!
interface FastEthernet0/3
description Telefono&PC
switchport access vlan 60
switchport mode access
switchport voice vlan 1001
no ip address
!
```

Como se señaló anteriormente esta configuración depende de la VLAN a la cual corresponda asignar cada uno de los puertos, y se debe seguir estos parámetros para la configuración del resto de equipos de conmutación Cisco.

5.2.1.3- Configuración de VLAN Trunks

El enlace troncal provee de un método eficaz para distribuir la información del identificador de VLAN a otros switches. Para realizar la configuración se

establece a un puerto como un enlace troncal. Los enlaces troncales soportan diferentes tipos de trunking, sin embargo para este caso en particular se utilizará el modo *trunking* que coloca a la interfaz en un modo permanente de trunking y negocia para convertir el enlace en un enlace troncal, esto se lo realiza mediante el comando *switchport mode trunk*, y posteriormente se selecciona el tipo de encapsulación. Los dos tipos de encapsulación existentes son el Inter-Switch-Link (ISL) e IEEE 802.1Q. Por motivos de compatibilidad con las versiones del resto de equipos se empleará la encapsulación 802.1Q. Los pasos a seguir para la configuración de puertos que enlacen hacia otros switches son:

Cuadro 5.7 : Pasos para configurar una interfaz como tipo trunk en los switches Cisco.

Parámetro a configurar	Comando
Ingresar al modo de configuración	configure terminal
Ingresar a un puerto del switch	interface fastEthernet *puerto-id* **/** gigabitEthernet *puerto-id*
Setear la interfaz como trunking	switchport mode trunk
Seleccionar encapsulacion IEEE802.1Q	switchport trunk encapsulation dot1q
Salir de la configuración	end
Verificar el puerto configurado	show running-config

De esa manera las interfaces configuradas como trunk permitirán transportar tráfico para cualquier VLAN.

5.2.1.4- Configuración de enrutamiento entre VLANs

Habitualmente la utilización de VLANs implica que únicamente los usuarios miembros de una misma VLAN puedan comunicarse, sin embargo dado que en este caso lo que se busca es reducir los dominios de broadcast, la comunicación debe ser posible entre todas VLANs. Para realizar el enrutamiento entre VLANs es indispensable un router o un switch de capa 3.

El switch de core de PETROCOMERCIAL Quito, Cisco Catalyst 4500 [1], es un equipo de conmutación capa 3 y será por lo tanto el equipo a cargo de cumplir las funciones de enrutamiento. Este equipo dada su alta capacidad, realiza el enrutamiento a velocidades equivalentes a la conmutación, sin provocar latencia al efectuar el enrutamiento.

Para que los switches Catalyst realicen el enrutamiento entre VLANs se deben crear interfaces de capa 3. Una interfaz capa 3 puede ser de tres tipos: *routed port [2], SVI(Switch virtual interfaces)[3] , y etherchannel port channel [4]*, en este caso se utilizará el concepto de Interfaz virtual del switch ***SVI***, dado que esta es la interfaz capa 3 definida por defecto para switches. La configuración de una SVI consiste en asignar una dirección IP y máscara de red a las VLANs determinadas, siendo esta dirección IP la correspondiente a la puerta de enlace de cada una de las VLANs. Como se observó en la configuración básica de los switches anteriormente, en el switch de core, Cisco Catalyst 4500, ya han sido asignadas las direcciones respectivas.

Previo al enrutamiento entre VLANs, es esencial de igual manera analizar que todos los equipos involucrados manejen el mismo tipo de encapsulación, en este caso el IEEE 802.1Q.

El siguiente paso consiste en habilitar el enrutamiento en el equipo a través de comando **ip routing**, como se muestra a continuación:

Pco_Roc_P50(config)# ip routing

A continuación se debe revisar que el comando este habilitado:

[1] La información técnica sobre el equipo Cisco Catalyst 4507 se le puede visualizar en el Anexo C.
[2] **Routed port:** es un puerto físico configurado como un puerto de capa 3, comando (**no switchport)**
[3] SVI(Switch virtual interfaces): es una interfaz VLAN, es por defecto una interfaz capa3.
[4] **EtherChannel port channel** en modo Capa 3: es una interfaz lógica port-channel ligada a la interfaz Ethernet dentro del channel group.

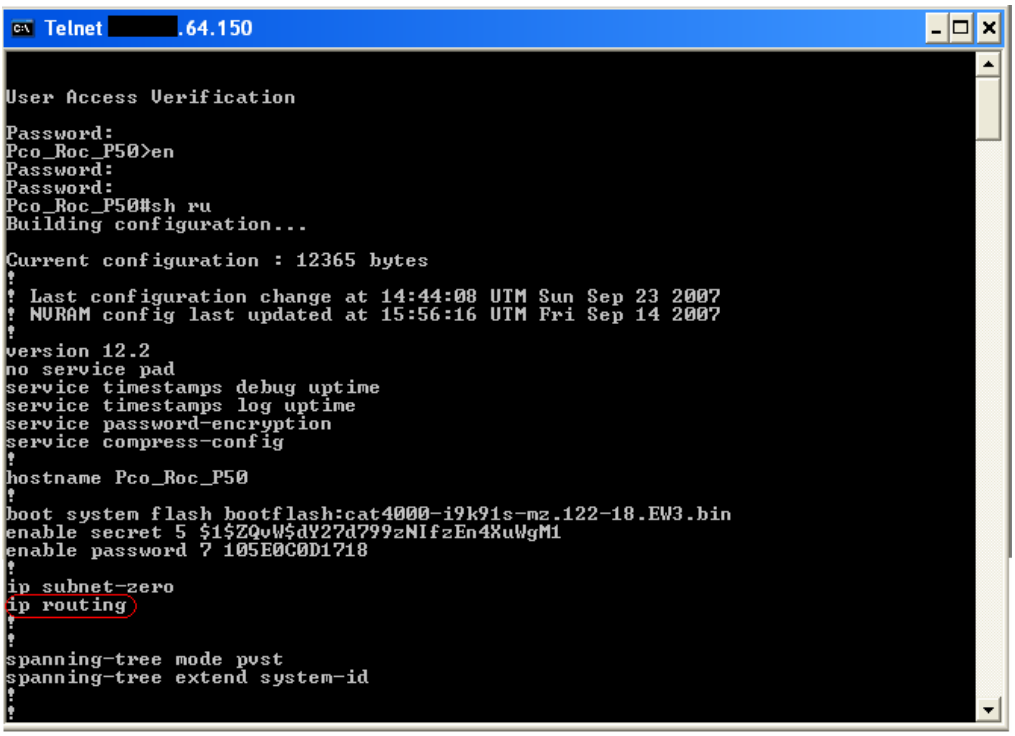


Figura 5.4: Pantalla de habilitación de enrutamiento en el Switch Pco_Roc_P50

Posteriormente es necesario establecer una ruta estática de salida para la red local, es decir para que los equipos puedan ingresar a la red WAN de PETROCOMERCIAL, para esto determinará que todo del tráfico que necesite salir de la red local lo haga a través del Router central de PETROCOMERCIAL Quito, un equipo Motorola *Vanguard 7310*, con dirección IP X.Y.64.11. Dado que cualquier tráfico interno saldría a la red WAN a través de este equipo se enrutará a este tráfico mediante una ruta estática, para lo cual se utiliza el comando **ip route.** La ruta estática se definiría entonces de la siguiente manera:

Pco_Roc_P50(config)# ***ip route 0.0.0.0 0.0.0.0 X.Y.64.11***

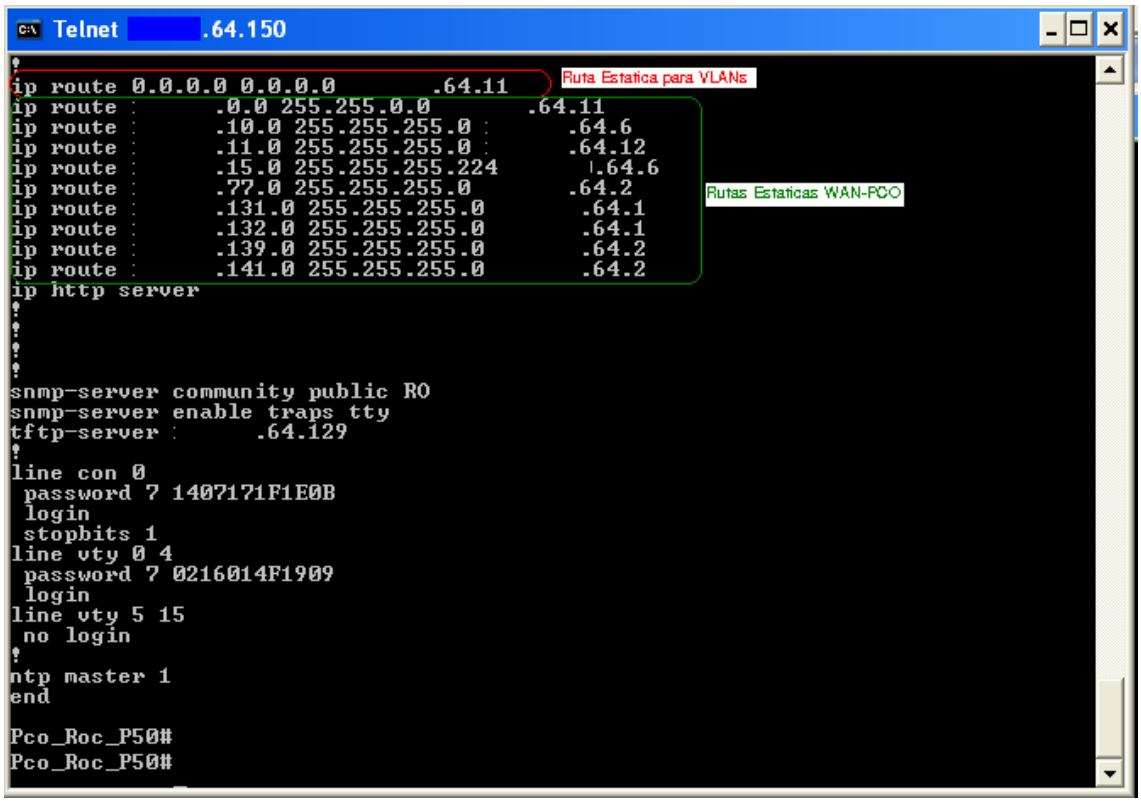


Figura 5.5: Pantalla de configuración de enrutamiento en el Switch Pco_Roc_P50

Finalmente el último paso consiste en configurar los equipos finales para que utilicen la puerta de enlace respectiva, de acuerdo a su interfaz VLAN a la cual pertenecerían. Por citar un caso, si un equipo pertenece a la VLAN 20, este equipo requiere que se configure como su puerta de enlace a la dirección IP de la puerta de enlace de la VLAN 20, la dirección X.Y.64.33, de no establecerse esta dirección IP el equipo podría relacionarse exclusivamente con el resto de host miembros de la misma VLAN y no estaría en capacidad de comunicarse con el resto de la red LAN y WAN de la empresa.

La configuración de los equipos finales se la hace en cada una de las tarjetas de red de los mismos equipos, como se visualiza en la siguiente figura:

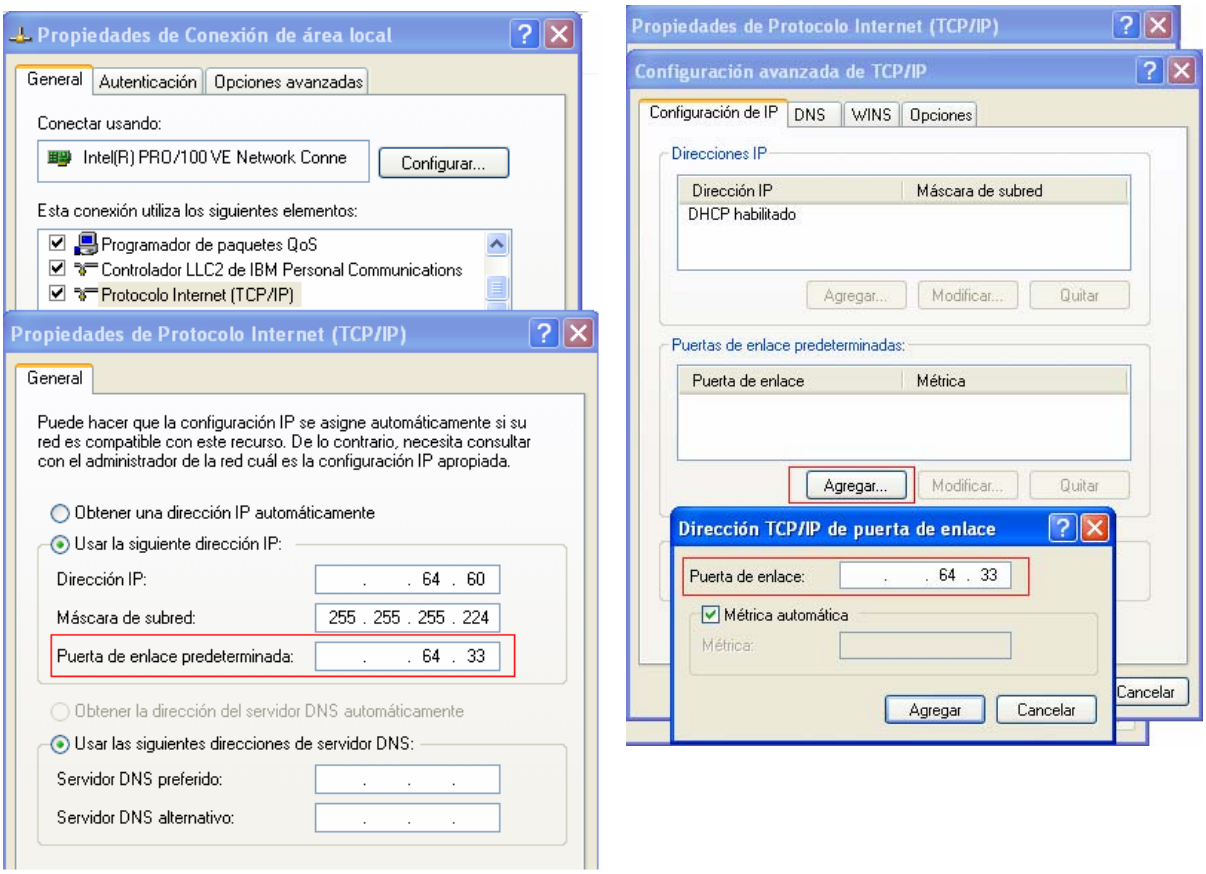


Figura 5.6: Configuración del direccionamiento IP en las PCs

5.2.1.5- Configuración de VTP

La configuración de VTP mantiene la configuración de VLAN de manera unificada en todo un dominio administrativo de red común, reduciendo la complejidad de la administración y el monitoreo de redes con VLANs.

Previa a la configuración de VTP se deben analizar tres aspectos importantes:

- ✓ Determinar el número de versión del VTP que se utilizará.
- ✓ Determinar si este switch será miembro de un dominio de administración que ya existe o si se deberá crear un nuevo dominio. Si un dominio de administración ya existe, determinar el nombre y la contraseña del dominio.
- ✓ Elegir un modo VTP para el switch.

La versión que de VTP que se utilizará es la **versión 2**, puesto que es la mas actual soportada por todos los switches incorporados en la red local. En cuando al dominio de administración se creará un dominio nuevo, actualmente no se hace uso del protocolo VTP en la empresa. El dominio VTP de PETROCOMERCIAL Quito, se denominará **PCOQuito.**

El switch de core de la empresa, será el encargado de la propagación de las VLANs creadas en el mismo, por lo que únicamente este switch funcionará con modo ***VTP Server*** (Servidor) lo que provocará la propagación de VLANs a los switches conectados al mismo y cuyo modo VTP sea ***VTP client*** (cliente). Por lo tanto el switch principal funcionará como servidor, mientras el resto de equipos funcionarán como clientes. No se establecerá clave para el dominio VTP, en el caso de que la empresa lo considere necesario, se lo implementará.

Además se habilitará la función ***VTP Pruning*****.** VTP pruning es un sistema que permite a los switches añadir o eliminar dinámicamente VLANs a los trunks, creando una red mucho mas eficiente. Para la configuración de VTP, analizada previamente, en el switch principal se deben seguir los siguientes pasos:

Cuadro 5.8 : Pasos para habilitar y configurar VTP en los switches Cisco.

Parámetro a configurar	Comando
Ingresar al modo de configuración de VTP	vlan database
Habilitar la version 2 de VTP	vtp version 2
Habilitar VTP pruning	vtp pruning
Establecer como modo Servidor	vtp **server**
Establecer el nombre del dominio	vtp domain ***PCOQuito***
Salir de la configuración	end
Verificar la configuración VTP	show vtp status

Para la configuración de VTP en el resto de switches cisco, la configuración varía únicamente en el modo de VTP, como se muestra en el cuadro a continuación:

Cuadro 5.9 : Pasos para configurar el modo VTP en los switches Cisco.

Parámetro a configurar	Comando
Ingresar al modo de configuración de VTP	vlan database
Habilitar la version 2 de VTP	vtp version 2
Habilitar VTP pruning	vtp pruning
Establecer como modo Servidor	vtp **client**
Establecer el nombre del dominio	vtp domain ***PCOQuito***
Aplicar los cambios	apply
Salir de la configuración	end
Verificar la configuración VTP	show vtp status

Nota: Es importante revisar que todos los switches se encuentren en modo ***transparent*** (transparente) previo a la configuración de VTP, puesto que si existe más de un switch con modo VTP Server, podrían generarse conflictos en la red.

A continuación se muestra la configuración del switch principal y de uno de los switches de la red de PETROCOMERCIAL Quito:

Configuración del switch de core, Cisco Catalyst 4507:

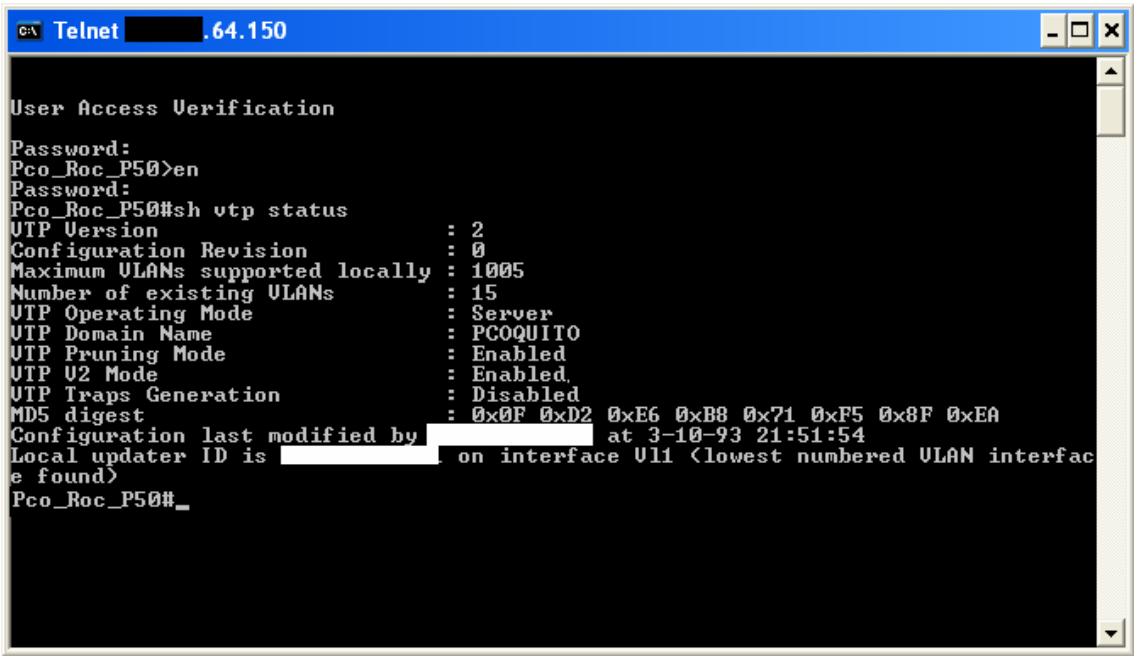


Figura 5.7: Pantalla de configuración de VTP en el Switch Pco_Roc_P50

Conjuntamente se describe la configuración completa del equipo:

Pco_Roc_P50#show vtp status

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 1005

Number of existing VLANs : 15

*VTP Operating Mode : **Server***

*VTP Domain Name : **PCOQuito***

*VTP Pruning Mode : **Enabled***

*VTP V2 Mode : **Enabled***

VTP Traps Generation : Disabled

MD5 digest : Configuration last modified by 172.20.64.150 at 0-0-00 00:00:00

Configuración de un switch Cisco Catalyst 3560:

Figura 5.8: Pantalla de configuración de VTP en el Switch Pco_Roc_P01

Conjuntamente se describe la configuración completa del equipo:

Pco_Roc_P01#show vtp status

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 1005

Number of existing VLANs : 15

*VTP Operating Mode : **Client***

*VTP Domain Name : **PCOQUITO***

*VTP Pruning Mode : **Enabled***

*VTP V2 Mode : **Enabled***

VTP Traps Generation : Disabled

MD5 digest : 0x86 0xA8 0xAF 0xE8 0x42 0xFD 0xBC 0xB3

Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

5.2.1.6- Configuración de Spanning-Tree

El protocolo Spanning-Tree se encarga de calcular una topología optima de la red, deshabilitando enlaces redundantes y levantándolos en caso de ser necesario. Para la red de PETROCOMERCIAL Quito se habilitará el modo **PVST+**[1] , el cual es el modo spanning-tree utilizado por defecto en los puertos ethernet. Este modo se utilizará dado que no todas las versiones de switches existentes en la red soportan un modo superior. Este modo debe ser habilitado en todos los equipos de conmutación, aunque por defecto ya se encuentra habilitado. La sintaxis del comando utilizado para configurar el modo spanning-tree es: **spanning-tree mode {** *pvst/mst /rapid-pvst* **}**.

- ✓ PVST (Per VLAN Spanning Tree) trabaja sobre cada una de las VLAN del switch, asegurando que cada una de ellas tenga una ruta en la red libre de bucles.
- ✓ MST(MST (Multiple Spanning Tree) optimiza el ambiente conmutado reduciendo el número de instancias STP I y el tráfico de BPDUs.
- ✓ Rapid PVST (Rapid-Per-VLAN-Spanning Tree) provee menor tiempo de convergencia a través del comando RSTP (Rapid Spanning Tree Protocol)[2].

El switch de core se configuraría entonces de la siguiente manera:

*Pco_Roc_P50(config)#**spanning-tree mode pvst***

[1] PVST+ (Per VLAN Spanning Tree) :Spanning-Tree por VLAN
[2] RSTP (Rapid Spanning Tree Protocol): Fue especificado en IEEE 802.1w, es una evolución del Spanning tree Protocol (STP), reemplazándolo en la edición 2004 del 802.1d. RSTP reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología.

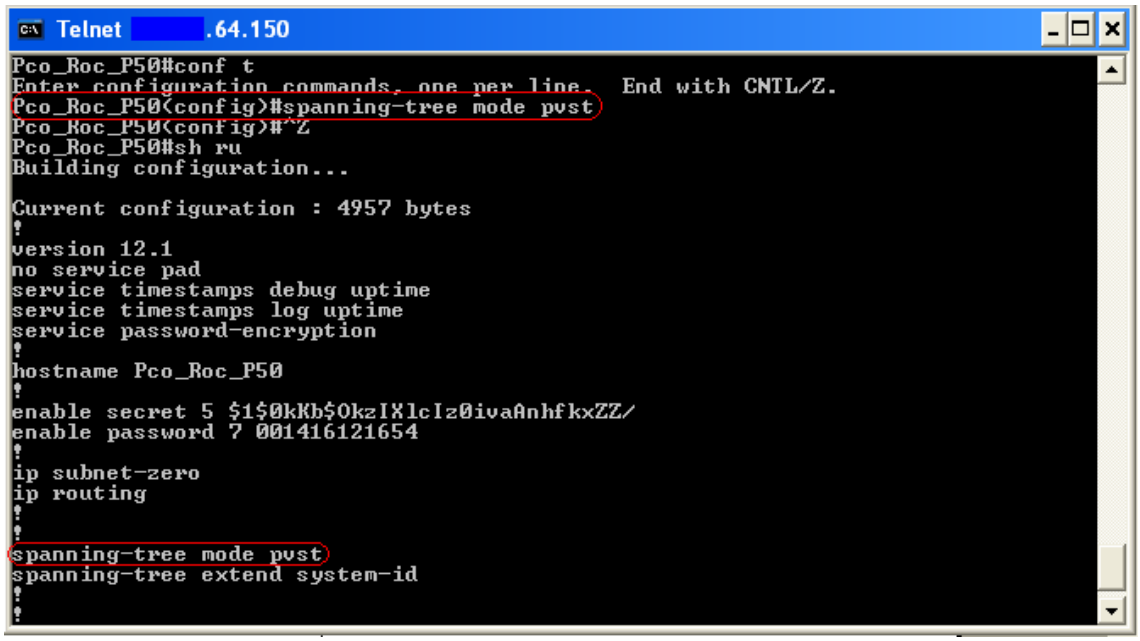


Figura 5.9: Pantalla de configuración de Spanning-Tree en el Switch Pco_Roc_P50

El siguiente paso es la selección y configuración del switch raíz. Para el caso de PETROCOMERCIAL Quito, el switch que corresponde para ser seleccionado como puente raíz es el switch de core, puesto que se trata de una topología estrella, donde todos los switches convergen con este equipo, el mismo que administra a todas las VLANs. Ya seleccionado el switch raíz es necesario establecer la prioridad del mismo con un valor considerablemente bajo. La prioridad tiene un rango de 0 a 61400, en incrementos de 4096, por defecto el valor es 32768. En este caso se asignará un valor de 8192. Esta asignación debe configurarse para todas las VLANs del switch, de manera que este equipo sea el puente raíz de cada una de las topologías spanning-tree de las VLANs existentes. Para esto se utiliza el siguiente comando:

spanning-tree *vlan-id* **priority** *prioridad*

De manera que para configurar la prioridad a todas las VLANs, se configura de la siguiente manera:

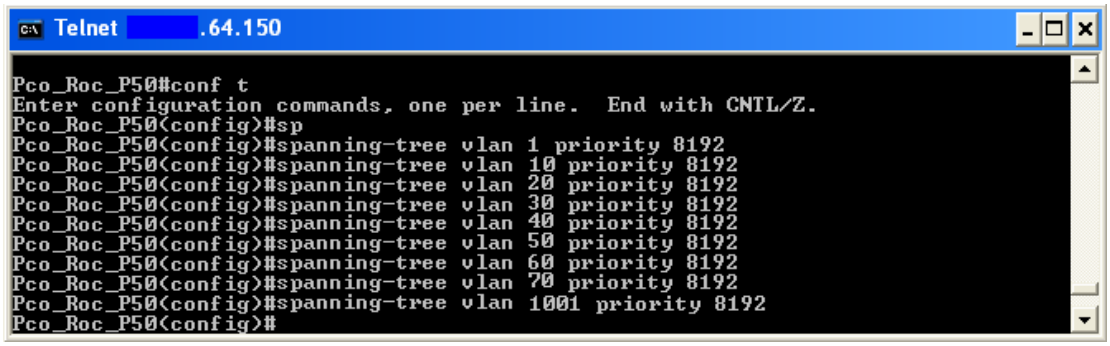


Figura 5.10: Pantalla de configuración de la prioridad de Spanning-Tree en el Switch Pco_Roc_P50

Conjuntamente se describe la configuración completa del equipo:

Pco_Roc_P50(config)#spanning-tree vlan 1 priority 8192

Pco_Roc_P50(config)#spanning-tree vlan 10 priority 8192

Pco_Roc_P50(config)#spanning-tree vlan 20 priority 8192

Pco_Roc_P50(config)#spanning-tree vlan 30 priority 8192

Pco_Roc_P50(config)#spanning-tree vlan 40 priority 8192

Pco_Roc_P50(config)#spanning-tree vlan 50 priority 8192

Pco_Roc_P50(config)#spanning-tree vlan 60 priority 8192

Pco_Roc_P50(config)#spanning-tree vlan 70 priority 8192

Pco_Roc_P50(config)#spanning-tree vlan 1001 priority 8192

Para verificar los cambios se utilizará el comando ***show spanning-tree.***

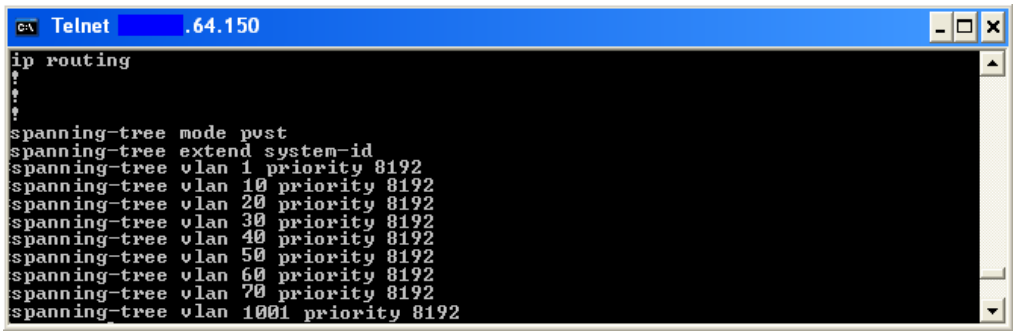


Figura 5.11: Pantalla de verificación de Spanning-Tree en el Switch Pco_Roc_P50

Normalmente el protocolo spanning-tree provoca retardo en todos los puertos al emprender el estado de iniciación de cada puerto, esto eventualmente puede provocar problemas en los puertos configurados como modos de acceso, debido a que toma de 30 a 50 segundos aproximadamente antes de que el switch pueda empezar a enviar el tráfico hacia un puerto. Para evitar esto se utiliza el comando portfast. Este comando al ser configurado en un puerto modo acceso, habilita a la interfaz a pasar desde el estado de **bloqueo**[1] al estado de **forward** [2] sin pasar por los estados intermedios, reduciendo al mínimo el tiempo de iniciación. Es por esto que el comando se lo utiliza exclusivamente en puertos conectados a dispositivos finales, de ser configurado en puertos conectados a hubs, concetradores, switches, bridges, entre otros, la interface podría causar bucles temporales al no pasar por todos los estados del protocolo spanning-tree.

El comando portfast se lo utiliza de la siguiente manera:

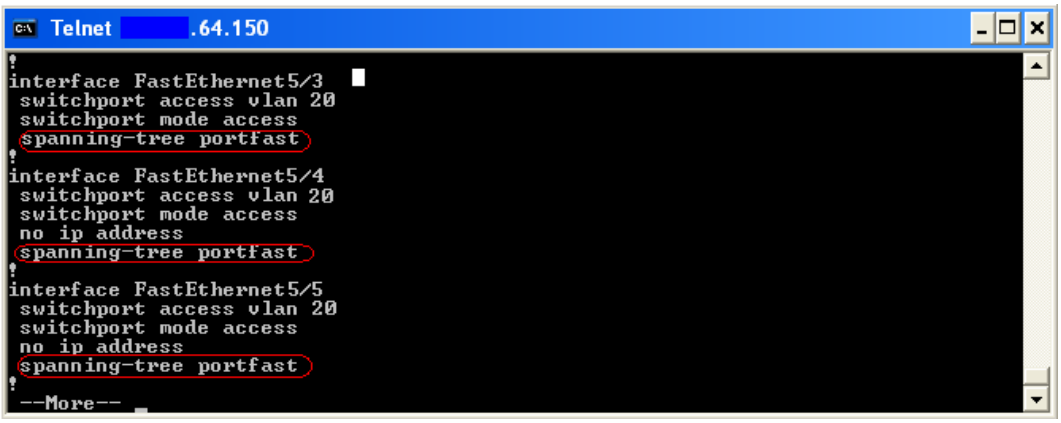


Figura 5.12: Pantalla de habilitación de Spanning-Tree en los puertos del Switch Pco_Roc_P50

[1] Bloqueo: Estado de STP donde el switch descarta paquetes de usuario, oye las BPDUs pero no aprende direcciones. Puede demorar hasta 20 segundos para cambiar al estado de escuchar.

[2] Forward (enviar):Estado de STP donde se envían datos de usuario y se aprenden direcciones MAC y procesan las BPDUs

Este comando es habilitado en todos los puertos conectados a PCs y teléfonos IP.

5.2.1.7- Configuración de Calidad de servicio

Una red con QoS se considera una red inteligente capaz de identificar y priorizar los tráficos críticos. La gran mayoría de redes pueden aprovechar los beneficios de la calidad de servicio (**QoS, Quality Of service**), sobre todo en el caso de este proyecto, en donde se debe dar importancia al manejo del tráfico de voz. La calidad de servicio es la aplicación de funcionalidades requeridas para manejar apropiadamente y satisfacer los requerimientos de las aplicaciones sensibles a pérdidas y retardo en su transmisión. QoS permite brindar preferencia a las aplicaciones consideradas como críticas, proporcionando prioridades.

El Cisco IOS[1] brinda soporte de calidad de servicio en base valores de clase de servicio (CoS[2]) del estándar IEEE 802.1p.

Para habilitar el Qos global en los switches se utiliza el comando mls qos, de la siguiente manera:

Pco_Roc_P50 #configure terminal

Pco_Roc_P50 (config)# ***mls qos***

[1] **Cisco I.O.S.:** es el sistema operativo que utilizan los equipos C**isco**,
[2] **CoS** (Class of Service): Clase de Servicio es un término que se utiliza para diferenciar el tráfico de una red.

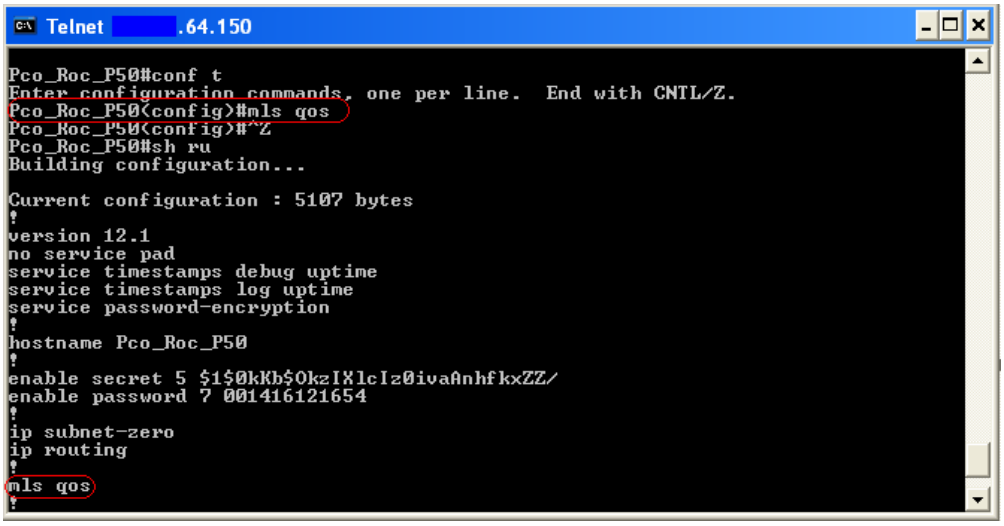


Figura 5.13: Pantalla de habilitación de QoS en el Switch Pco_Roc_P50

El nivel de prioridad normal abarca el rango de **0 a 4**, mientras las tramas con valor de prioridad de **5 a 7** son enviadas al encolamiento de alta prioridad. Se debe entonces configurar el estado de confianza del puerto. Dado que el tráfico de datos no tiene requerimientos especiales para QoS, es decir su prioridad de considera como normal, se establecerá su valor de clase de servicio en 0. Para configurar la QoS en una interfaz conectada únicamente a un dispositivo final, el puerto debe configurarse con el comando mls qos Cos 0, tal como se muestra a continuación:

Pco_Roc_P50 (config)*#interface fastethernet 5/3*

Pco_Roc_P50 (config-if)# **mls qos cos 0**

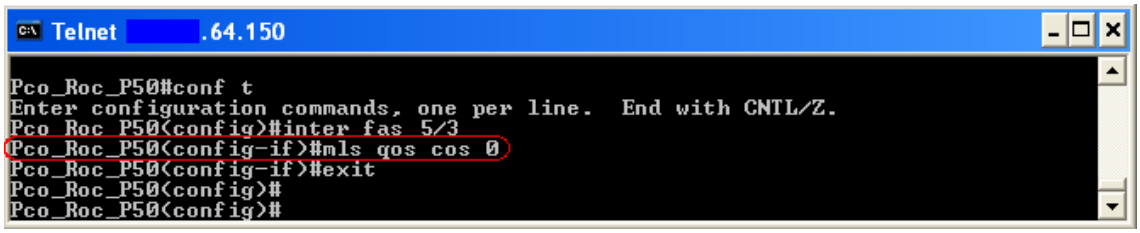


Figura 5.14: Pantalla de habilitación de QoS en los puertos a dispositivos finales en el Switch Pco_Roc_P50

Los teléfonos IP establecen automáticamente su campo de clase de servicio al conectarse a los equipos de conmutación. Los teléfonos IP “Mitel” se setean con un valor de 6, el cual es apropiado para el tráfico de voz (prioridad alta), lo que representa que se debe dejar el valor de la clase de servicio intacto, o en otras palabras se establece el estado de confianza del puerto en **confiar** (**trust**).

Para puertos conectados a teléfonos IP, se utilizó el comando mls qos trus cos, como se muestra a continuación:

Pco_Roc_P50 (config)*#interface fastethernet 7/11*

Pco_Roc_P50 (config-if)# **mls qos trust cos**

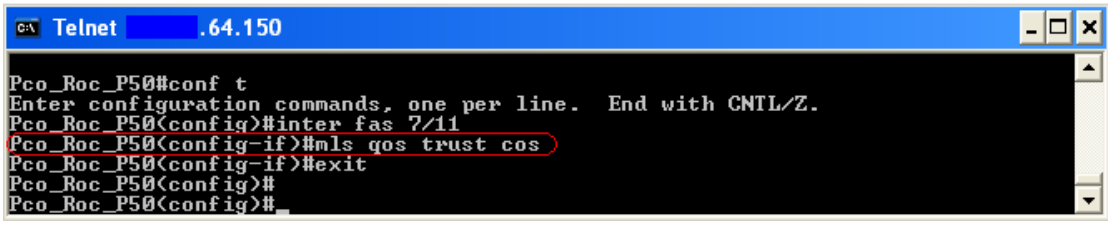


Figura 5.15: Pantalla de habilitación de QoS en los puertos a teléfonos IP en el Switch Pco_Roc_P50

Para verificar los cambios realizados se hace uso de este comando: **show mls qos interface.**

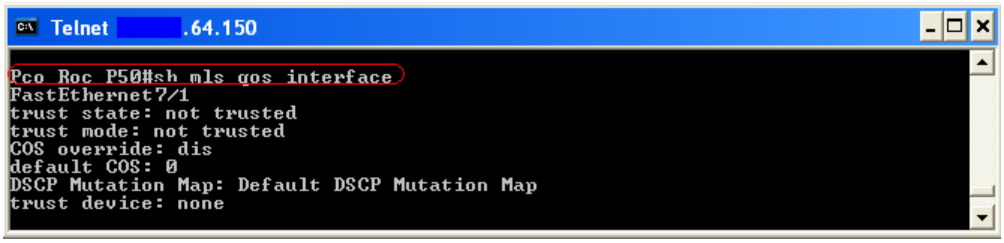


Figura 5.16: Pantalla del comando de verificación de QoS en el Switch Pco_Roc_P50

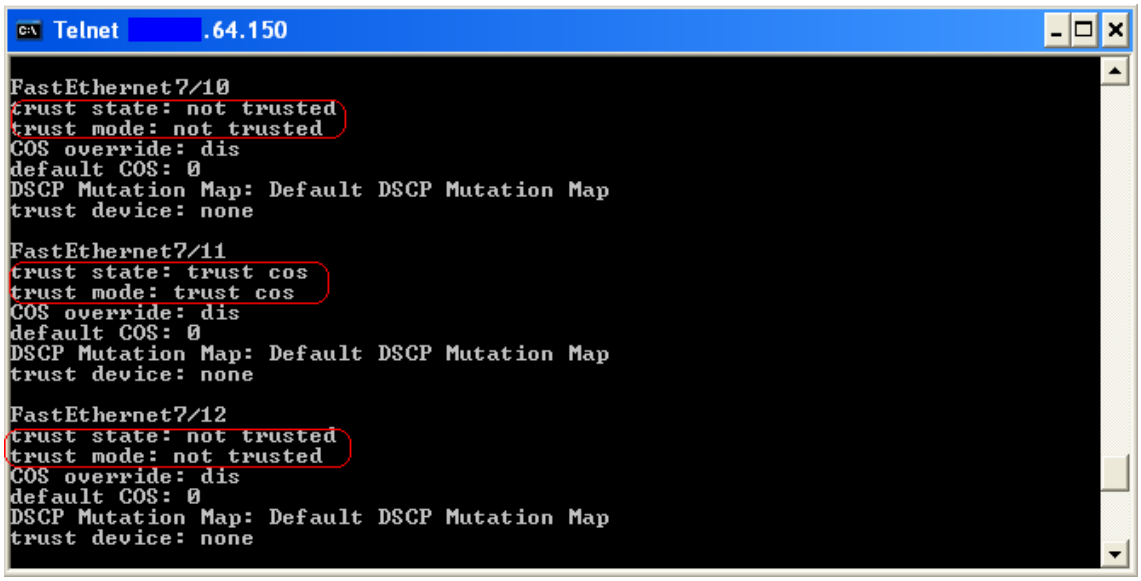


Figura 5.17: Pantalla de verificación de QoS en el Switch Pco_Roc_P50

La calidad de servicio asegurará a la red de PETROCOMERCIAL Quito que el tráfico de voz y datos no sea ni perdido ni retardado, añadiendo fiabilidad y disponibilidad, brindando a los usuarios tiempos de respuesta más rápidos.

5.2.2- Central Telefónica IP MITEL

La configuración de la central telefónica IP se mantendrá intacta en cuanto al manejo de sus características generales. Exclusivamente se reestablecerá el direccionamiento IP del equipo, así como la configuración del DHCP del controlador.

El controlador Mitel 3300, provee de DHCP a los teléfonos IP, de manera que en el equipo se requiere establecer un rango de direcciones IP para el funcionamiento de los teléfonos IP, los cuales pertenecerán a la VLAN de voz.

5.2.2.1- Configuración de la dirección IP de la Central Telefónica IP

Para modificar el direccionamiento de la central telefónica IP Mitel, es preciso establecer una conexión serial con el controlador.

Al reestablecerse el direccionamiento del equipo, las configuración restante no se eliminará ni se modificará, únicamente se actualizará junto con los cambios que se realicen al resto del equipo.

Para establecer una conexión serial con el controlador, se utilizará un cable serial RS-232 desde el puerto de mantenimiento del controlador hacia el puerto serial de la PC con la que se proceda a trabajar. Es necesario indicar previo a la configuración la PC debe estar en la misma subred que la central IP. Además es recomendable obtener un respaldo del equipo en el caso de que se presenten inconvenientes luego de realizar la configuración.

Los pasos a seguir para reestablecer el direccionamiento IP del controlador son:

- ✓ Iniciar el programa de comunicación en la PC. (Hyper Terminal por ejemplo).
- ✓ Resetear al equipo, presionando el botón Reset del controlador (parte frontal del equipo).
- ✓ Una vez que el equipo haya sido reseteado se mostrará en el programa el texto " ***[VxWorks Boot]:*** " se ingresa el comando "***c***", seguido de la tecla *INTRO*.

Para ingresar los nuevos valores se digita el texto en frente del parámetro a cambiar, el siguiente cuadro detalla los parámetros de configuración que se presentarán:

Cuadro 5.10 : Parámetros iniciales a configurar de la Central Telefónica IP Mitel

Prompt	Valor	Descripción
boot device	ata=0,0	El dispositivo de arranque, es el disco
unit number	0	Número de unidad (No utilizado)
processor number	0	Numero de procesador (No utilizado)
file name	**: /partition1/Rtc8260**	Localización de archivo de inicio y el nombre del archivo (depende del equipo)
inet on Ethernet (e)	**Ejm:192.168.1.1:ffffff00**	**Dirección IP y máscara de red (en hexadecimal) para el controlador**
host inet (h)		Dirección IP de PC, utilizado para actualizaciones de software.
gateway inet (g)	**Ejm:192.168.1.2**	**Dirección IP de la puerta de enlace del controlador, no puede estar en el rango de DHCP distribuido por el mismo.**
user (u)	ftp	
ftp password (pw)	ftp	
flags (f)		Dirección IP fija, utilizada sobre el E2T para el DHCP.
other (o)		Otros dispositivo, E2T usado desde network boot

A continuación se muestra la configuración en sí, aplicando la información anterior:

boot device : ata=auto
unit number : 0
processor number : 0
file name : /partition1/Rtc8260
inet on ethernet (e) : 172.20.70.2:fffffe
host inet (h) : 0
gateway inet (g) : 172.20.70.1
user (u) : ftp
ftp password (pw) : ftp
flags (f) : 0x0
other (o) : motfcc

Posterior a los cambios se debe reiniciar el controlador, actividad que tomará entre 15 a 20 minutos, y finalmente cerrar la sesión y desconectar el enlace entre el controlador y la PC.

A partir de esta configuración, es recomendable establecer el resto de parámetros del equipo, a través de la interfaz web del equipo, la cual permite manejar la configuración de manera más ágil. Para ingresar a dicha interfaz, se hace uso de un browser (Internet Explorer por ejemplo), en el que se ingresa el nuevo direccionamiento IP en la barra de inicio.

Al ingresar al equipo se mostrará la siguiente pantalla:

Figura 5.18: Pantalla de inicio Central Telefónica Mitel

Se ingresa el nombre de usuario y la contraseña (definidos por default) y se ingresa al modo de configuración.

El siguiente paso es la configuración del resto de parámetros de direccionamiento IP, así como la configuración del DHCP del controlador.

5.2.2.2- Configuración de la Central Telefónica IP vía browser

Para ingresar al modo de configuración del controlador se selecciona la opción ***"Herramientas de administración del Sistema"***, en la pantalla inicial de opciones del controlador, como se visualiza a continuación:

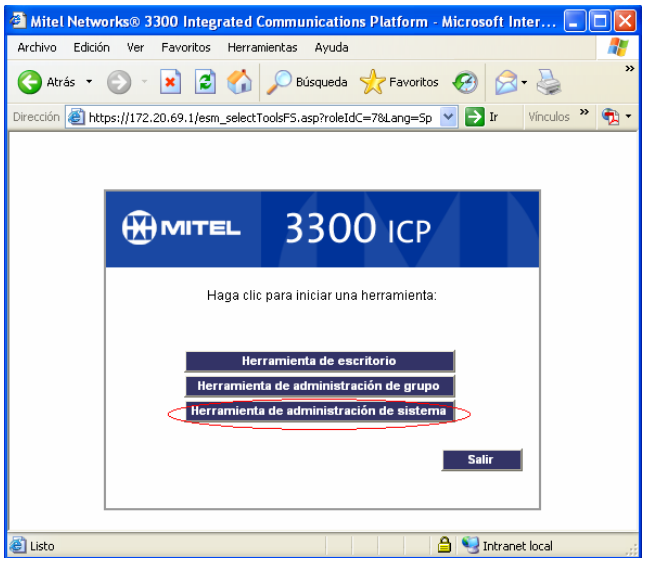


Figura 5.19: Pantalla de opciones de la Central Telefónica IP Mitel

En la pantalla de configuración se realizarán los cambios que sean pertinentes para realizar el redireccionamiento IP del equipo. La pantalla que se expondrá será la siguiente:

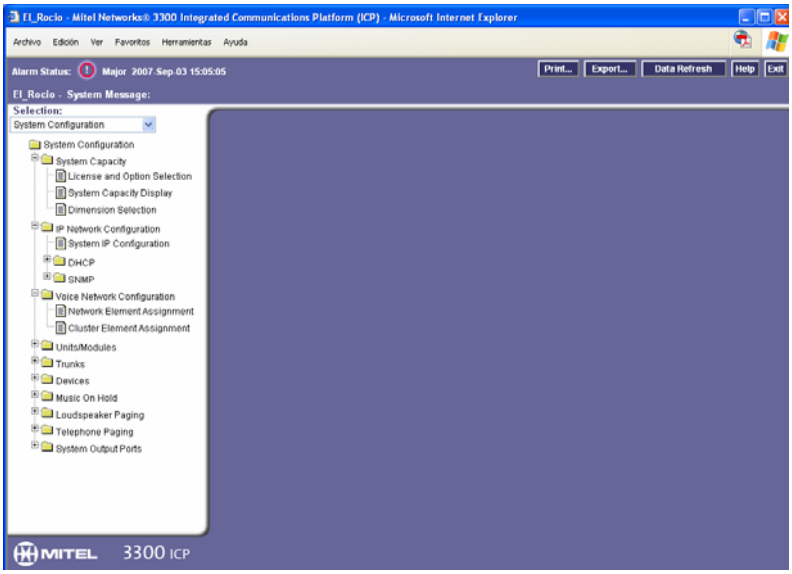


Figura 5.20: Pantalla inicial de modo de configuración del Controlador

El siguiente paso constituye la configuración de los parámetros de direccionamiento, para esto se ingresa en la opción *System Configuration* / *IP Network Configuration,* la opción ***System IP Configuration***. Aquí deben desplegarse los valores ingresados por consola a excepción de la puerta de

enlace (Gateway IP Address), la cual debe tomar el valor de la puerta de enlace de la VLAN de Voz, siendo esta, la X.Y.71.1.

El E2T[1] (Ethernet a TDM) es un parámetro significativo de configurar en el controlador, puesto que se utiliza la dirección IP asignada a E2T para la comunicación con Andinatel (troncales analógicas). Este parámetro se lo configurará posteriormente a la determinación de los rangos de DHCP.

Aceptando los cambios explicados anteriormente, la configuración se mantendría de la siguiente manera:

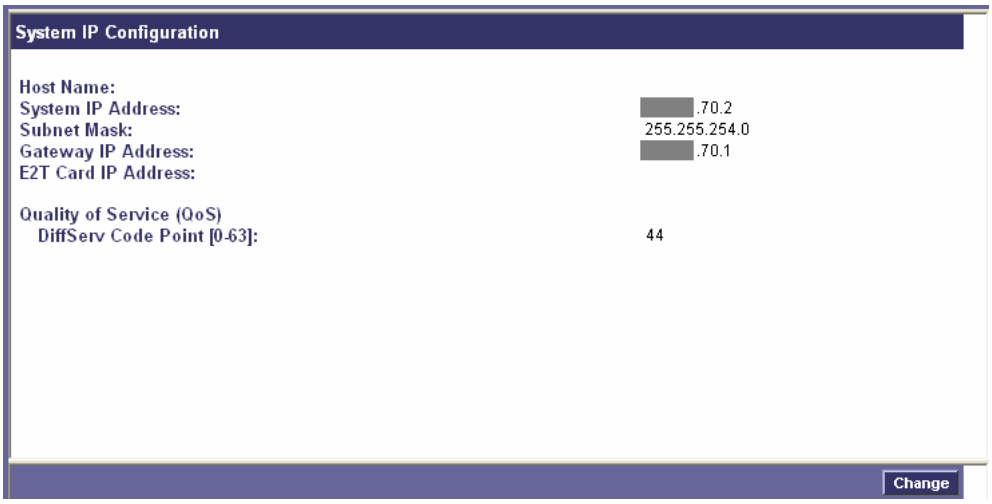


Figura 5.21: Pantalla de configuración del Sistema IP[2]

El siguiente paso es verificar que el servidor DHCP del controlador se encuentre autorizado, esta comprobación se la realiza en la opción ***DHCP Server*****,** habilitando el DHCP interno de la central telefónica Mitel, como se muestra en la siguiente figura:

[1] **E2T:** Ethernet a TDM(Time Division Multiplexing), tiene 64 canales de Ethernet para Multiplexión de división de tiempo.
[2] Las figuras han sido alteradas por motivos de confidencialidad de la empresa.

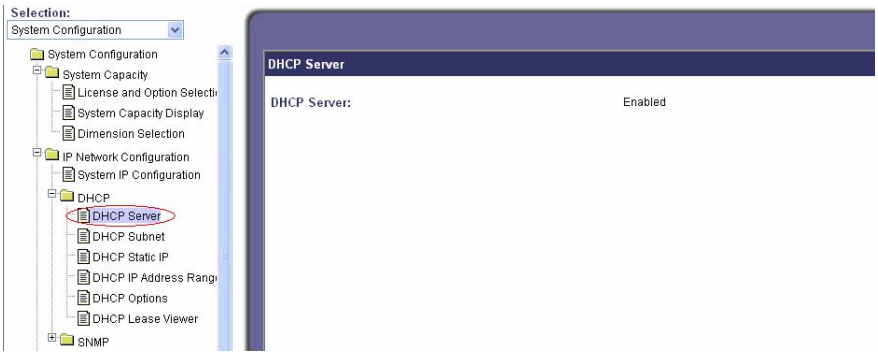


Figura 5.22: Activación del servidor DHCP la Central Telefónica Mitel

A continuación se requiere establecer el rango de direccionamiento IP que será asignado para el funcionamiento de DHCP en los teléfonos. Para esto es necesario determinar la subred correspondiente. Se ingresa en la opción *System Configuration* / *IP Network Configuration* / *DHCP,* la opción ***DHCP Subnet.*** En esta opción se ingresa la dirección de red y la máscara de la subred a la que pertenecerán los teléfonos IP. Por lo tanto se establecerá como dirección de red : X.Y.70.0 con máscara 255.255.254.0. A esta subred se la denomina **Rocio.**

La pantalla de configuración de la subred para el DHCP de los teléfonos IP es la siguiente:

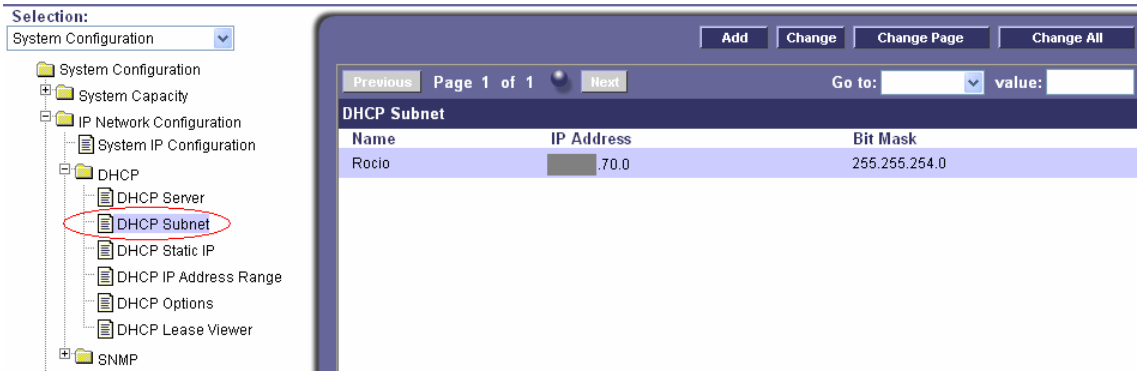


Figura 5.23: Subred asignada para DHCP de la Central Telefónica Mitel

Ya definida la subred, es necesario establecer la dirección IP de E2T. Para esto se debe seleccionar una dirección IP fija dentro del rango de la subred.

La dirección a asignarse será la X.Y.70.3, de forma consecutiva a la dirección del controlador. Para realizar este cambio se ingresa a la opción *System Configuration* / *IP Network Configuration* / *DHCP* la opción ***DHCP Static IP.***

Esta configuración se muestra en la siguiente figura:

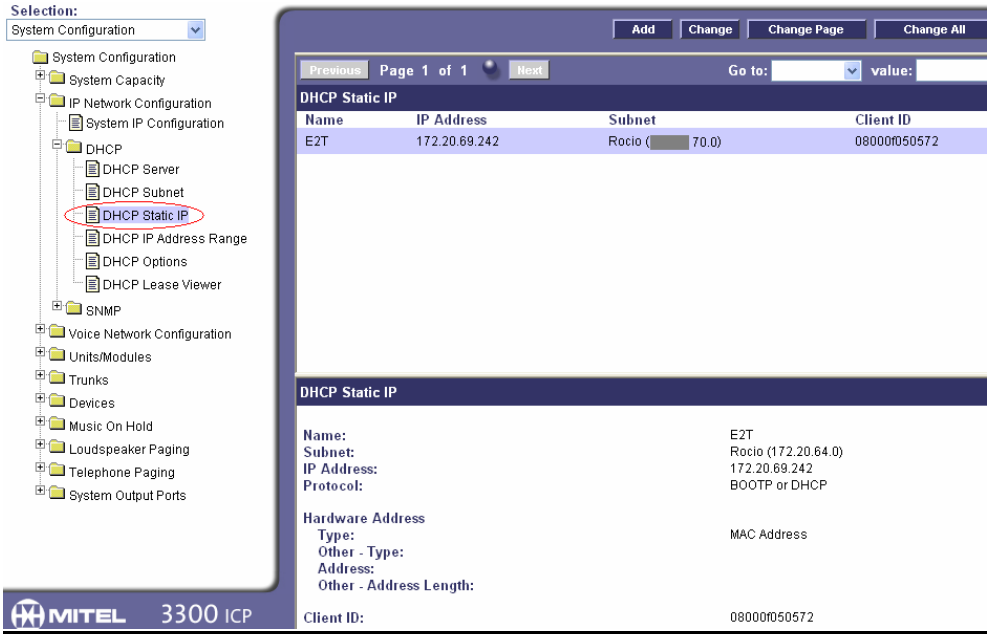


Figura 5.24: Asignación de E2T para la Central Telefónica Mitel

Con estas asignaciones es posible entonces realizar la configuración de inicio y final del direccionamiento IP para los teléfonos IP. En otras palabras se establecerá desde y hasta cual dirección IP se asignará a los teléfonos IP. Para esto se selecciona la subred ya creada y se establece el inicio y fin del rango.

El rango se determinará para iniciar en la dirección IP: X.Y.70.5 hasta la dirección IP: X.Y.71.254, abarcando aproximadamente la totalidad de la subred asignada a la VLAN de Voz. La siguiente figura muestra el resultado de esta configuración:

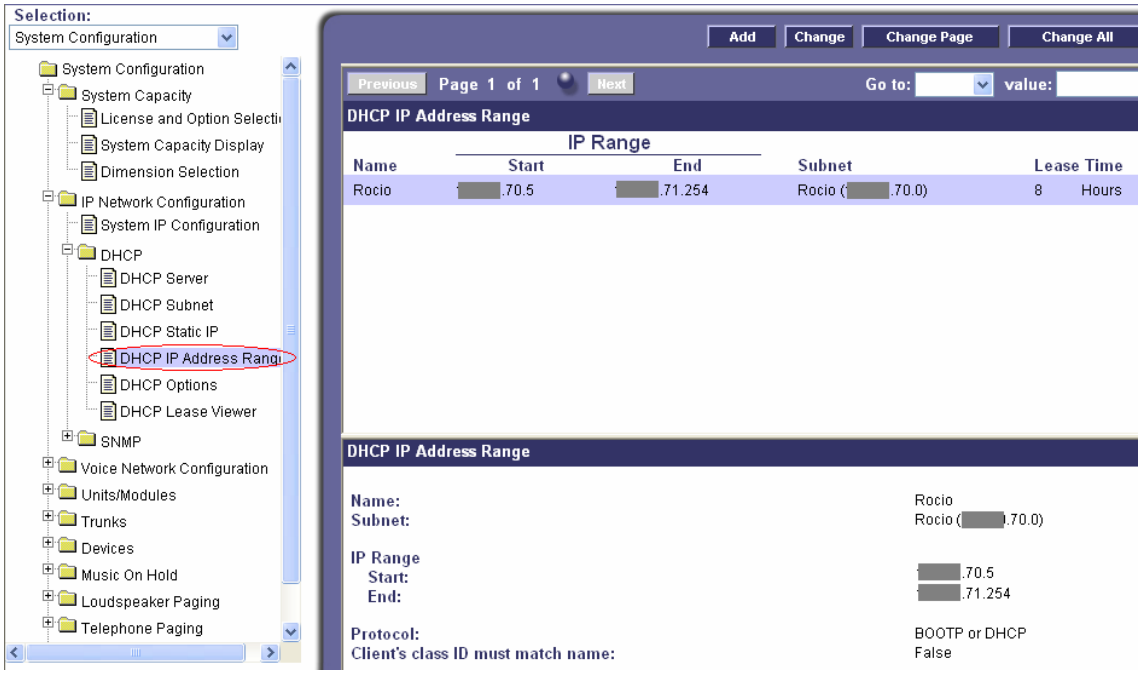


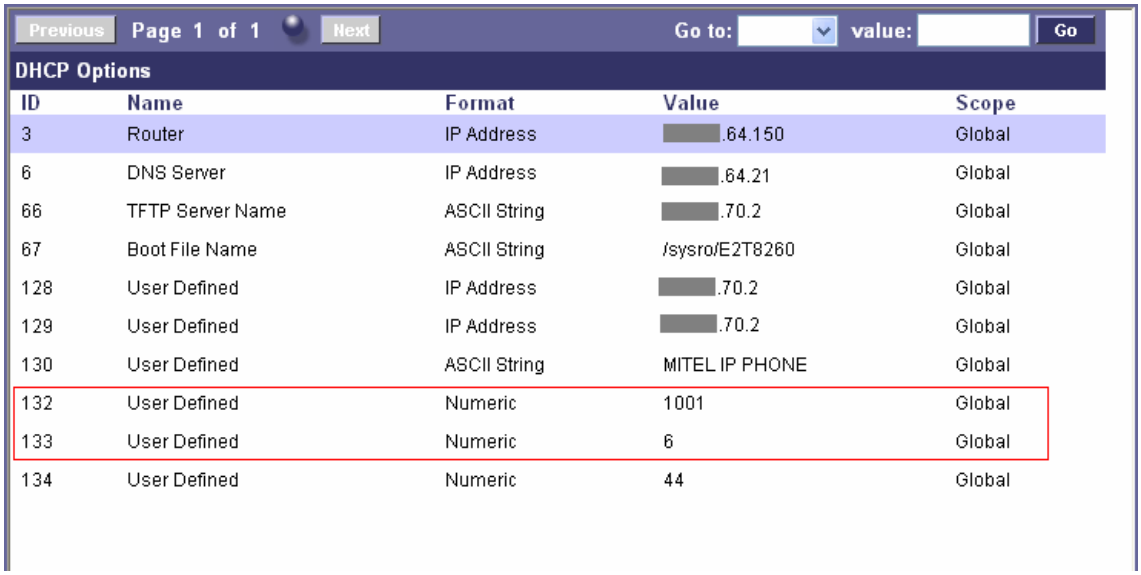
Figura 5.25: Rango de direccionamiento IP para el DHCP de la Central Telefónica Mitel

Finalmente es necesario establecer el ID de la VLAN de voz en la central telefónica IP, puesto que de esta manera los teléfonos IP y el controlador mismo sabrán a que VLAN pertenecen además del nivel de prioridad para la calidad de servicio. Para configurar estos dos parámetros es necesario basarse en la siguiente tabla de opciones para el DHCP del controlador:

Cuadro 5.11 : Tabla de configuración de las opciones DHCP del controlador

ID Opción	Valor
3	Dirección IP del default gateway
6	Dirección IP del servidor DNS
66	Servidor TFTP con formato ASCII String
67	TFTP BootFile(archivo de arranque)
128	Servidor TFTP con formato IP address
129	RTC con formato IP address
130	Servidor DHCP (Valor por defecto: ASCII String=MITEL IP PHONE)
132	VLAN ID para la VLAN de voz(Hex - 32 bit/ Numeric)
133	Prioridad (Valor 1 al 7 , MITEL recomienda 6)

Las opciones que se configurarán corresponden a las opciones **132** y **133**. La configuración se muestra a continuación:


Previous Page 1 of 1 Next Go to: value: Go

DHCP Options

ID	Name	Format	Value	Scope
3	Router	IP Address	[redacted].64.150	Global
6	DNS Server	IP Address	[redacted].64.21	Global
66	TFTP Server Name	ASCII String	[redacted].70.2	Global
67	Boot File Name	ASCII String	/sysro/E2T8260	Global
128	User Defined	IP Address	[redacted].70.2	Global
129	User Defined	IP Address	[redacted].70.2	Global
130	User Defined	ASCII String	MITEL IP PHONE	Global
132	User Defined	Numeric	1001	Global
133	User Defined	Numeric	6	Global
134	User Defined	Numeric	44	Global

Figura 5.26: Opciones DHCP de la Central Telefónica Mitel

Nota: RTC (Real Time Complex) es usado para la señalización de los teléfonos IP y también el DHCP, TFTP, entre otros. entre los teléfonos IP y el RTC son enviados el progreso de la llamada, el estatus del dispositivo y mensajes de actualización.

5.2.3- Configuración de DHCP

PETROCOMERCIAL Quito opera un servidor DHCP Windows 2003 Server, este equipo será el que se encargará de la asignación dinámica de las direcciones IP a todas los computadores de la red local. Debido a la presencia de las VLANs se requiere por tanto la creación de rangos de direccionamiento IP (**scopes**) para cada una de la VLANs establecidas para la red de PETROCOMERCIAL Quito.

El Servidor DHCP identifica a las VLANs para asignarles sus respectivas direcciones IP basándose en la puerta de enlace o gateway de cada una de ellas, a través de las cuales se ingresan las peticiones DHCP (requests). Es

decir que el servidor reconoce a que VLAN pertenece cada computador de acuerdo a su puerta de acceso y a partir de esto asigna una dirección dinámica perteneciente a la VLAN que corresponde al equipo.

Los pasos a seguir para la creación de rangos o scopes en el servidor DHCP Windows 2003 Server son:

En la pantalla de configuración del servidor, y se elige la opción ***New Scope*****,** presionando el botón derecho del mouse sobre el nombre del servidor (**pcored01.petrocomercial.com)** como se muestra en la siguiente figura:

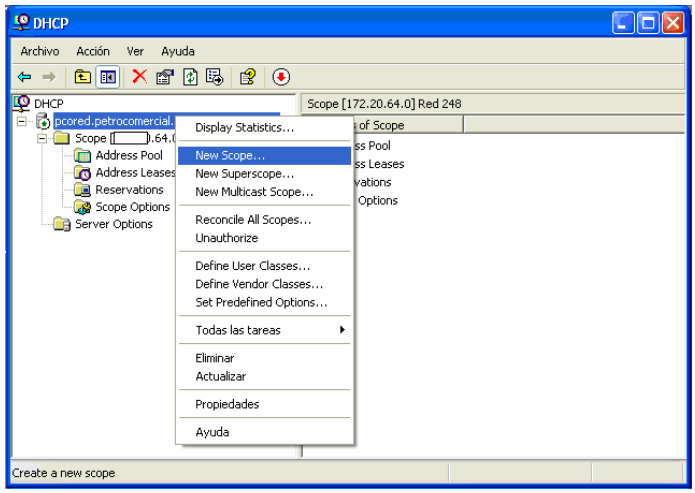


Figura 5.27: Pantalla de configuración del servidor DHCP

A continuación se deben completar los parámetros para la creación de un nuevo rango de acuerdo al asistente (wizard) de creación presentado por el servidor. La primera pantalla requiere el nombre y la descripción del rango. En este caso se mostrarán el rango definido para la VLAN 80 o VLAN Administrativa, como se muestra en la siguiente figura:

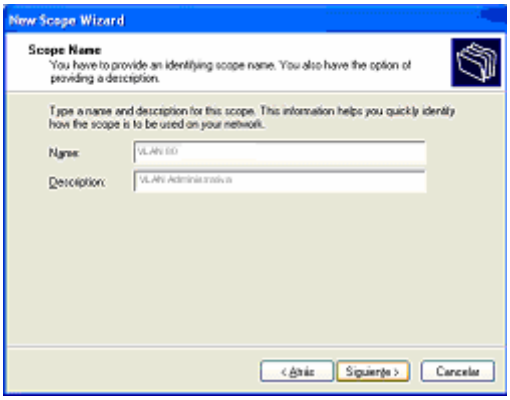


Figura 5.28: Asistente para la creación de un nuevo Scope

Luego se ingresa el rango de direcciones IP, la dirección IP inicial, la final, y la máscara de red a la cual pertenece la VLAN.

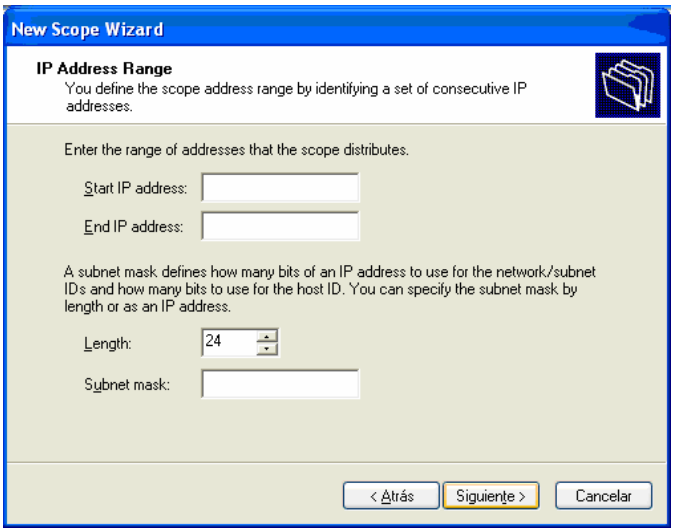


Figura 5.29: Definición del direccionamiento IP para el nuevo Scope.

Existe además la definición de exclusiones. Las exclusiones son direcciones IP o un rango de direcciones IP, que no serán distribuidas por el servidor, pero que no se requieren para el caso actual.

A continuación se detalla el tiempo que un cliente puede mantener su dirección IP dentro del *scope* definido (tiempo de arriendo).

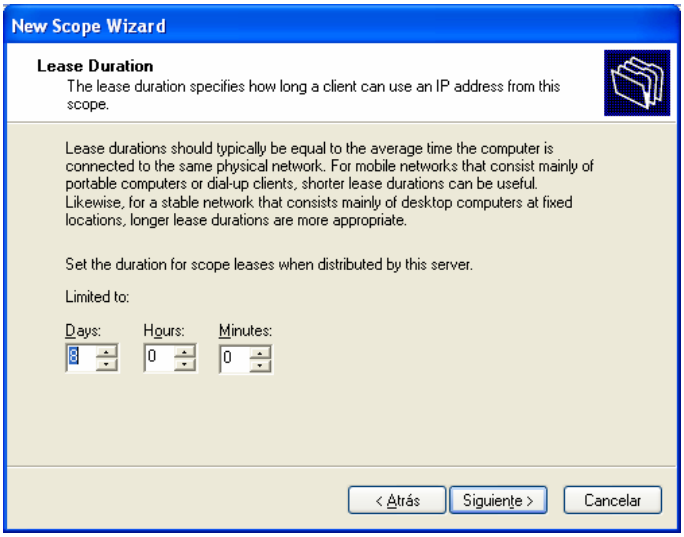


Figura 5.30: Definición del tiempo de arrendamiento para el nuevo Scope.

En la siguiente pantalla se ingresa la puerta de enlace o default gateway respectivo para el rango definido, es decir la puerta de enlace de la VLAN correpondiente para este scope. Para la VLAN 80, su puerta de enlace es la X.Y.68.1 , como se visualiza a continuación:

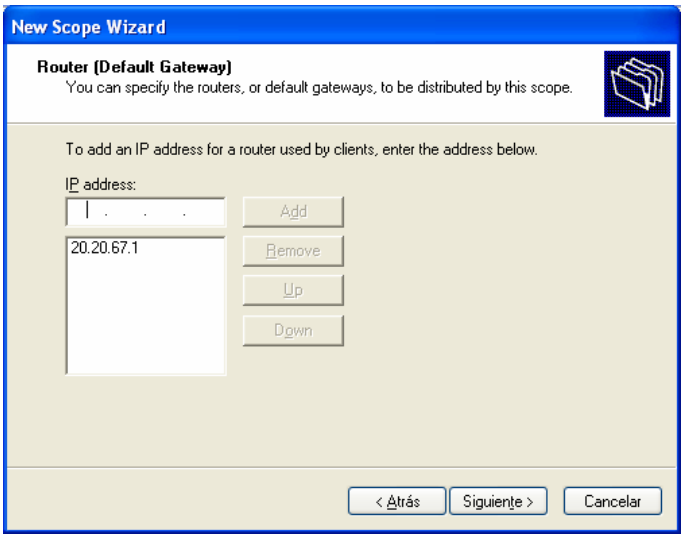


Figura 5.31: Definición de la puerta de enlace para el nuevo Scope.

Luego se digita el nombre del dominio de Petrocomercial, y el nombre y dirección IP del servidor DNS de la red, de acuerdo al direccionamiento IP ya determinado, como se muestra en esta figura:

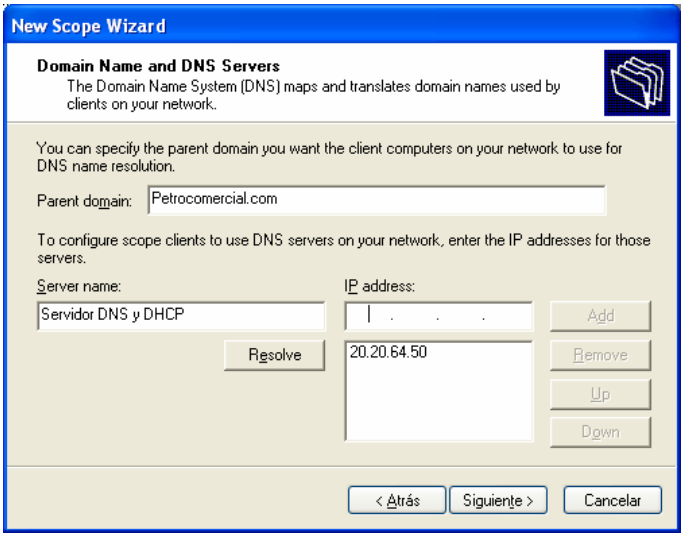


Figura 5.32: Definición del nombre de dominio para el nuevo Scope.

En la siguiente ventana se muestra la configuración de Servidores WINS, lo cual se deja intacto ya que no se cuenta con este tipo de servidores en la empresa.

Finalmente se puede activar el nuevo *scope* en ese momento, o se lo puede realizar posteriormente. Se selecciona activar en este momento y el servidor DHCP puede empezar a asignar direcciones IP de este rango a los equipos que pertenezcan a la VLAN 80.

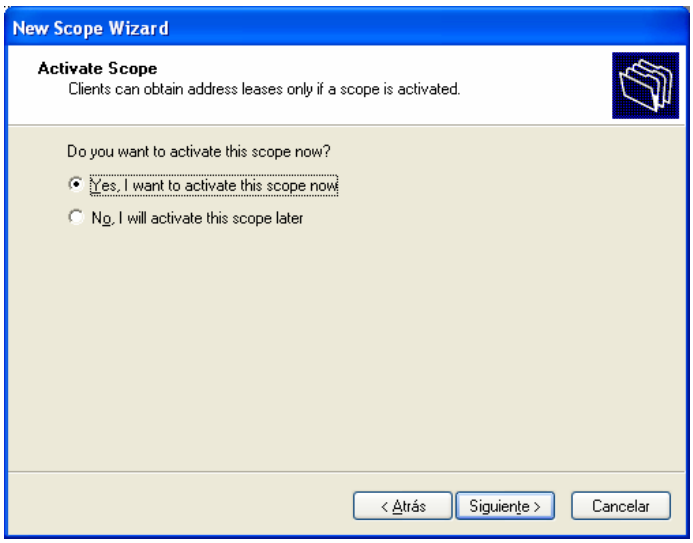


Figura 5.33: Activación del nuevo Scope.

Este proceso se lo realiza con las VLANs General, Usuarios de Sistemas, Industrial, Administrativa y Comercialización (1, 60, 70, 80 y 90).

Nota: En el servidor DHCP Windows 2003 Server existe la opción de crear direcciones reservadas, de forma que siempre se asigne la misma dirección IP al mismo equipo.

Una vez establecidos los rangos de DHCP para todas las VLANs, se debe determinar en cada una de las VLANs el direccionamiento IP del servidor DHCP, puesto que al no encontrarse el servidor dentro de cada uno de los grupos, los equipos no podrán direccionar al servidor, es por ello que se utiliza el comando **ip helper address**, en la definición SVI de las VLANs, de esta manera los equipos conocerán a que equipo solicitar una dirección dinámica.

Para utilizar este comando se ingresa a la interfaz de cada una de las VLANs cuyo direccionamiento sea dinámico, y se ingresa el comando seguido de la dirección IP del servidor DHCP de PETROCOMERCIAL Quito, el X.Y.64.21, tal como se muestra a continuación:

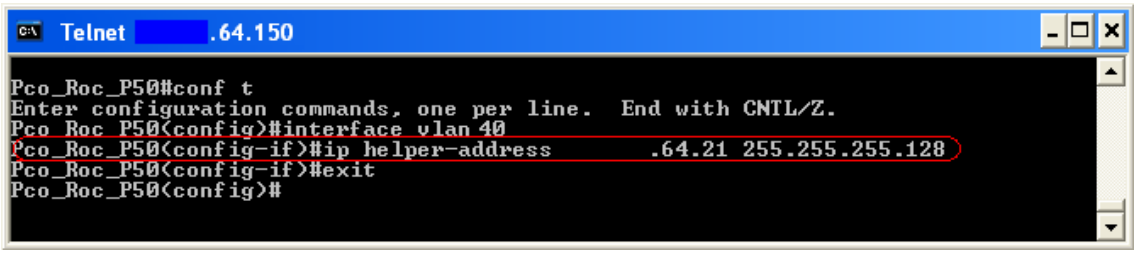


Figura 5.34: Pantalla del comando ip helper-address en el Switch Pco_Roc_P50

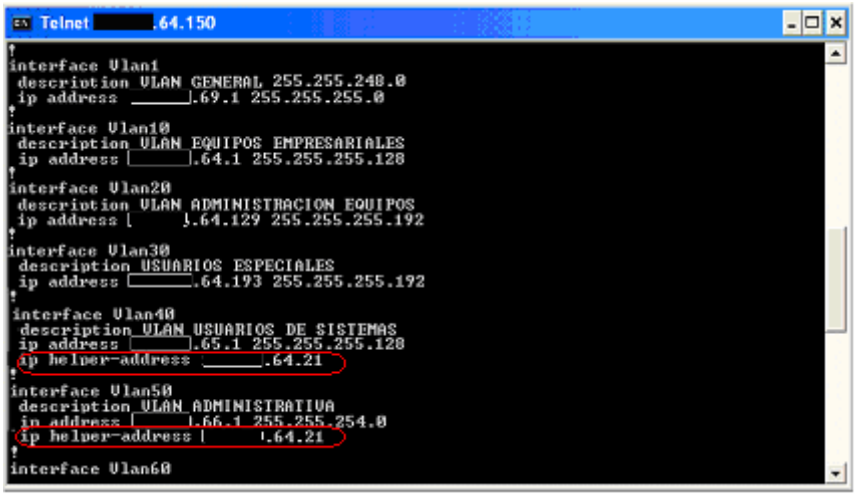


Figura 5.35: Pantalla de configuración del servidor DHCP para las VLANs en el Switch Pco_Roc_P50

5.2.4- Equipo de seguridad ASTARO

El equipo de seguridad perimetral ASTARO, provee varias aplicaciones de seguridad integradas. Para el actual proyecto se realizarán cambios exclusivamente en la administración de recursos (redes y servicios), y políticas de seguridad perimetral.

Astaro Security Gateway es configurado a través de su interface web. Para acceder al equipo es necesario autentificarse con un usuario registrado por el equipo.

En el menú principal se encuentran todas las opciones del equipo. En la opción ***Definitions*** (definiciones) se ingresan a las opciones que se configurarán, siendo estos: **redes y servicios**, como se visualiza en la siguiente figura:

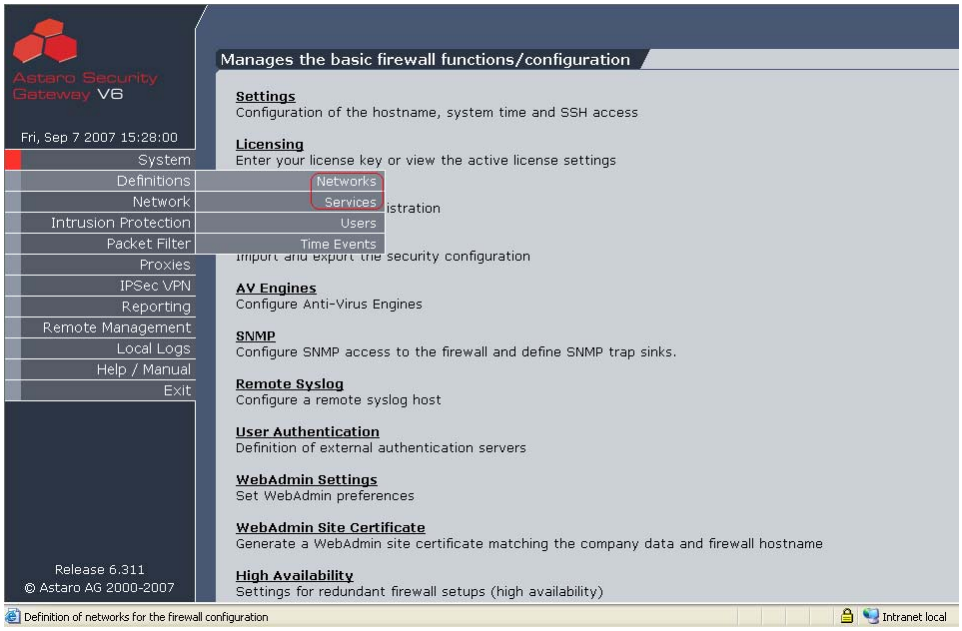


Figura 5.36: Menú Principal del equipo ASTARO.

Para la administración de políticas de seguridad se ingresa a la opción ***Packet Filter*** (filtrado de paquetes), seguido de la opción ***Rules*** (Reglas), como se muestra en la siguiente figura:

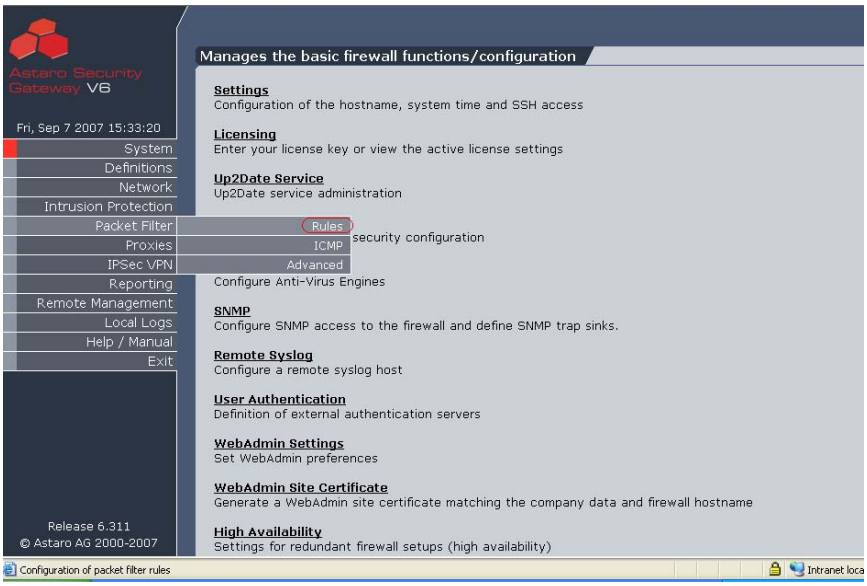


Figura 5.37: Menú Packet Filter del equipo ASTARO.

5.2.4.1- Administración de Redes (Networks)

Una red puede ser añadida, modificada o eliminada. En el equipo de seguridad perimetral Astaro, una red es un recurso que puede estar

conformado por un solo usuario, un grupo de usuarios, o una subred determinada. Para añadir una red se ingresa a la opción ***New Definition***, en la pantalla de administración de redes o ***Network Definitions***, como se muestra a continuación:

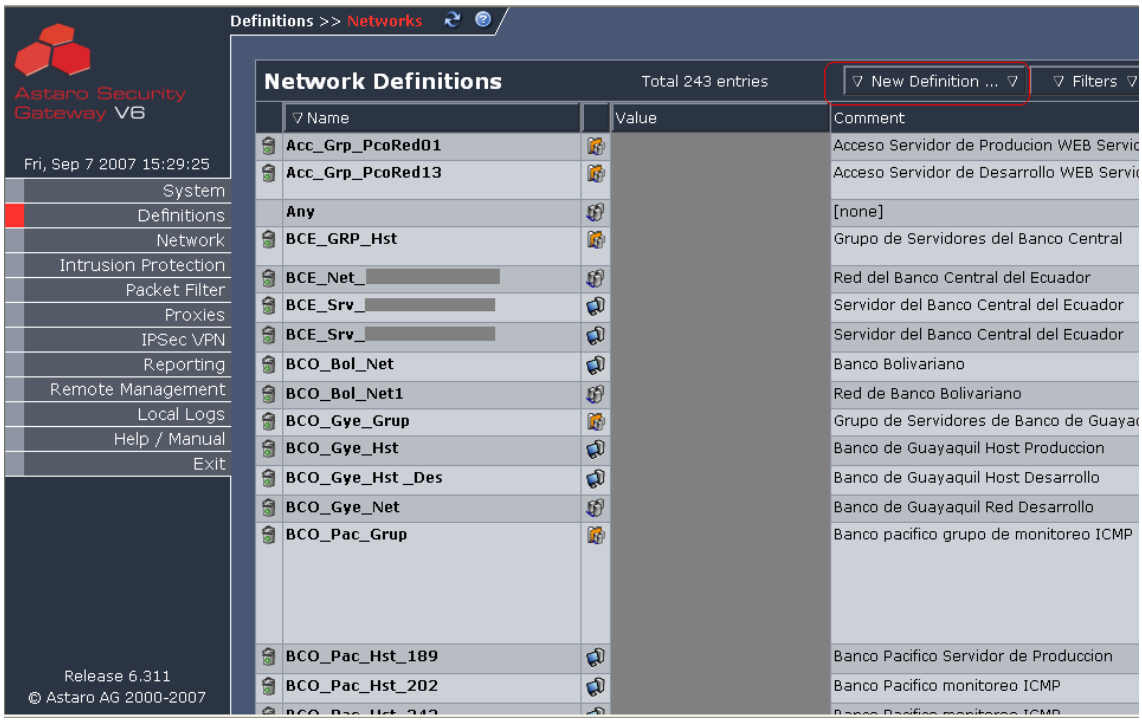


Figura 5.38: Menu Network Definitions del equipo ASTARO

En la pantalla siguiente se ingresa la información correspondiente a la nueva red que se desea crear, por mencionar un ejemplo la definición del grupo *Pco_Host_MEM*, analizada en el capítulo anterior. La siguiente figura muestra el ejemplo:

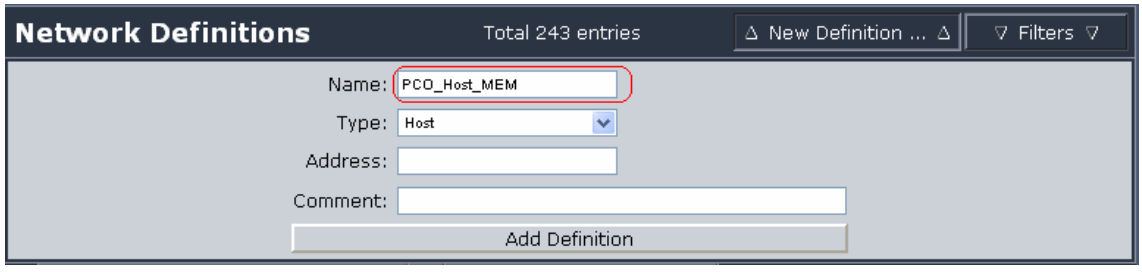


Figura 5.39: Creación de Network Definitions en el equipo ASTARO

Para modificar las redes definidas con anterioridad, se selecciona la red que será alterada y se realizan los cambios en la misma pantalla.

Este procedimiento se realizó con todas las políticas las cuales requerían de rectificaciones o de nuevas definiciones de sus recursos de red.

5.2.4.2- Administración de Servicios

Los recursos de servicios al igual que las redes pueden ser administradas, para esto se ingresa a la opción ***Service Definitions*** (Definiciones de Servicio). Posteriormente para ingresar a la definición de un nuevo servicio se ingresa a la opción ***New Definitions*** (Nuevas Definiciones), como se muestra a continuación:

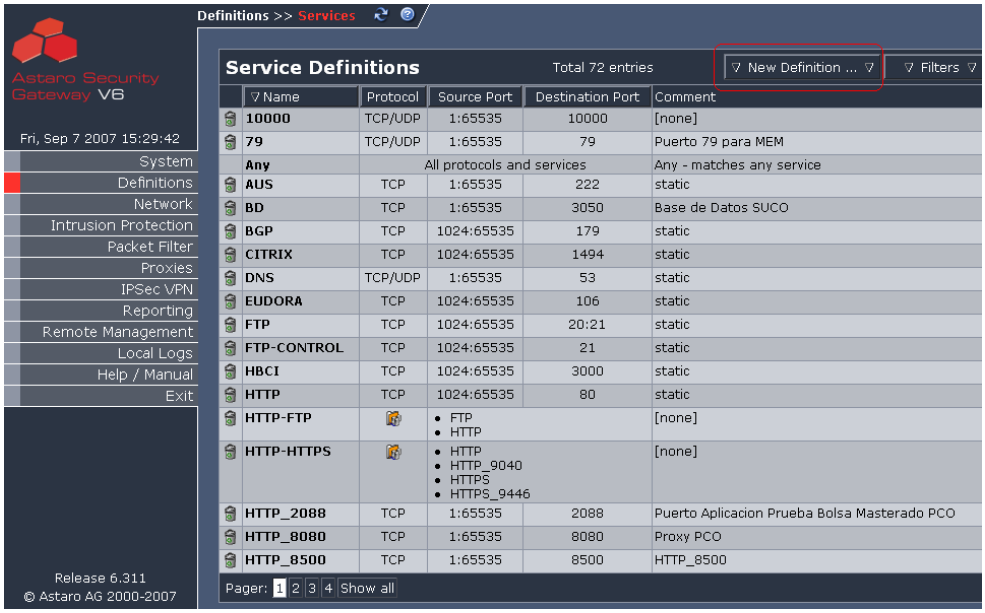


Figura 5.40: Menu Service Definitions del equipo ASTARO

En la siguiente pantalla se determina el servicio de acuerdo a lo requerido para el proyecto, como por ejemplo en el caso de la política 1 con tipos de servicio inexactos, se debe crear el servicio denominado Aplicaciones PEC que se muestra en el siguiente cuadro:

Cuadro 5.12 : Recurso de servicio agregado para la segunda parte de la propuesta para la Política 1 con tipos de servicio inexactos.

No.	Nombre	Protocolo	Puerto de origen	Puerto de Salida	Observaciones
1	**Aplicaciones PEC**	TCP	1:65535	**3050**	Base de Datos SUCO
		TCP	1:65535	**137:139**	Aplicaciones Contables

Para realizar esta configuración es necesario establecer inicialmente como servicio a todos componentes de este nuevo servicio, de esta manera se crea primero el servicio Aplicaciones Contables, de la siguiente manera:

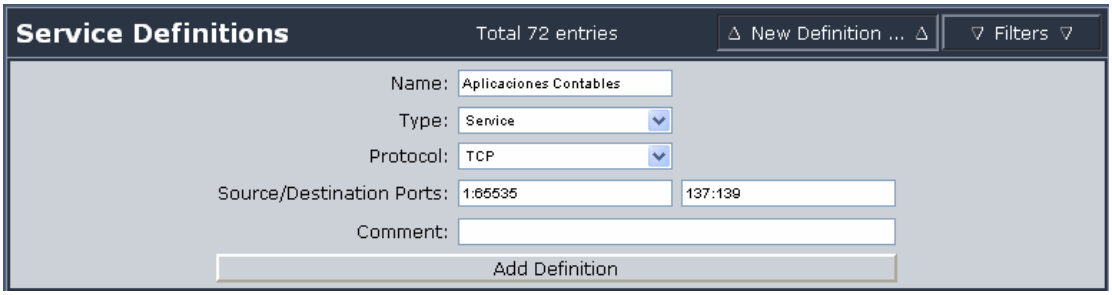


Figura 5.41: Creación de Service Definitions en el equipo ASTARO

Luego de que ambos componentes del servicio Aplicaciones PEC están determinados, se crea el servicio, seleccionando todos sus elementos (usando la tecla control), y finalmente se define el nuevo servicio como se muestra en la siguiente figura:

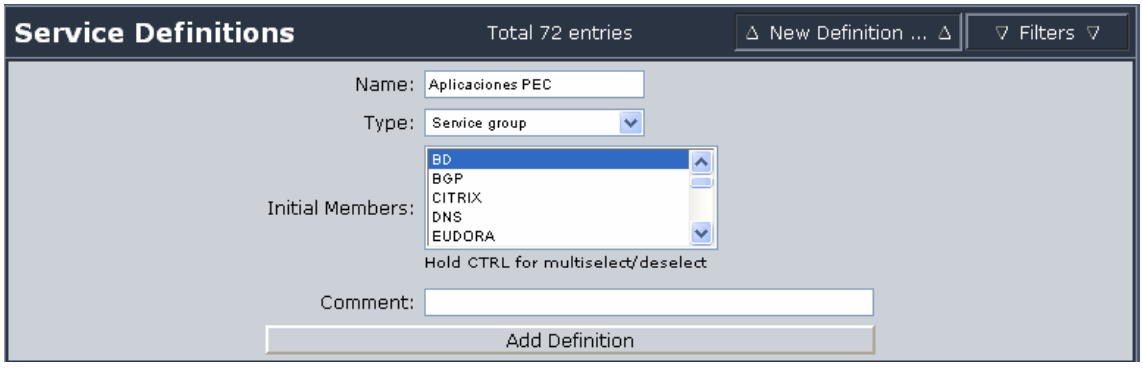


Figura 5.42: Creación de Service Definitions por grupos en el equipo ASTARO

En los casos en los que es necesario modificar un servicio, se selecciona el servicio que será alterado y se realizan los cambios en la misma pantalla.

Este procedimiento se realizó con todas las políticas las cuales requerían de rectificaciones o de nuevas definiciones de sus recursos de servicios.

5.2.4.3- Administración de Políticas

En la generación de políticas se hace uso de los recursos anteriormente definidos , es por ello que se hicieron las respectivas correcciones y adiciones en los recursos del equipo de seguridad, de manera que estos sean utilizados adecuadamente en la administración de políticas de seguridad de la empresa que requieren ser rectificadas.

Para crear una nueva política de seguridad se ingresa a la opción New Rule (Nueva Regla), como se muestra a continuación:

Figura 5.43: Menú Packet Filter del equipo ASTARO

En la siguiente pantalla se selecciona:

- ✓ Tipo de servicio (Recursos de servicio determinados anteriormente)
- ✓ La acción que se ejecutará (Permitir o Denegar)

- ✓ Grupos de origen y destino.
- ✓ Grupo al que pertenece la política y su posición dentro del grupo(Grupos lógicos)
- ✓ Comentario u observación (opcional).

La siguiente figura muestra la creación de la segunda parte de la política propuesta para la política 1 con tipos de servicio inexactos, como se detalla en el cuadro 5.13:

Cuadro 5.13 : Segunda parte de la propuesta para la Política 1 con tipos de servicio inexactos

Recurso	Origen	Servicio	Política	Destino	Descripción
PetroEcuador	Pco_Grp_UsEspeciales	**AplicacionesPEC**	Permitir	PEC_Grp_Net	Política para el acceso de usuarios autorizados hacia los servidores de las aplicaciones de PetroEcuador

Los parámetros se establecerían de la siguiente manera:

- ✓ Tipo de servicio: ***APLICACIONES PEC***
- ✓ La acción que se ejecutará: ***Permitir(allow)***
- ✓ Origen: ***Pco_Grp_UsEspeciales***
- ✓ Destino: ***Pec_Grp_Net***
- ✓ Grupo: ***Petroecuador***
- ✓ posición: ***Al inicio (to group top)***
- ✓ Comentario: ***Política para el acceso de usuarios autorizados hacia los servidores de las aplicaciones de Petroecuador.***

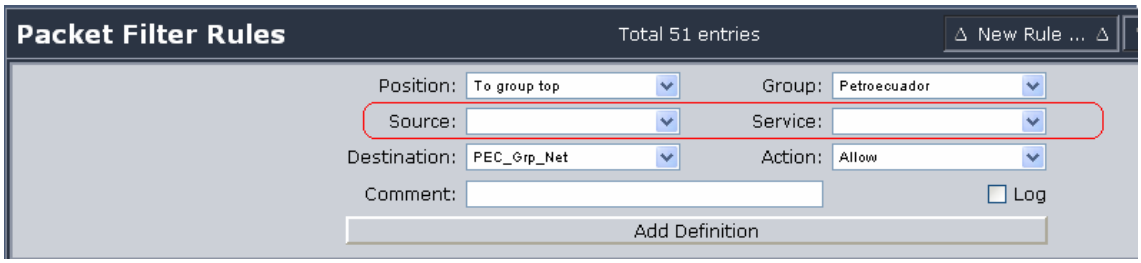


Figura 5.44: Creación de Packet Filter Rule en el equipo ASTARO

Para modificar una política que ya se encuentre definida, se selecciona el servicio que será alterado y se realizan los cambios en la pantalla de Packet Filter, como se muestra a continuación, donde se modifica la política 1 con tipos de servicio inexactos pero de acuerdo a la primera parte de la propuesta, estableciendo el servicio ***HTTP***, en lugar de cualquier servicio, como detalla el cuadro 5.14, reflejado en la siguiente figura:

Cuadro 5.14 : Primera parte de la propuesta para la Política 1 con tipos de servicio inexactos.

Recurso	Origen	Servicio	Política	Destino	Descripción
PetroEcuador	PCO_Net_UIO	**HTTP**	Permitir	PEC_Grp_Net	Política para el acceso al sitio Web de Petroecuador desde la red de PCO.

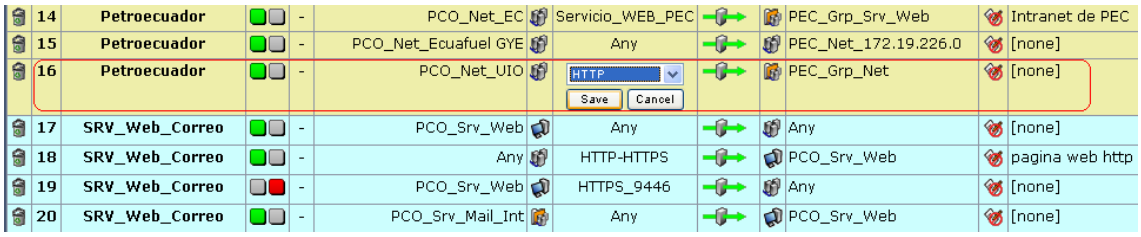


Figura 5.45: Modificación de Packet Filter Rule en el equipo ASTARO

El mismo procedimiento se lo realizó con el resto de políticas de seguridad que requerían ser rectificadas, de acuerdo a los análisis y propuestas establecidos en los capítulos anteriores.