ESCUELA POLITÉCNICA DEL EJÉRCITO

FACULTAD DE INGENIERIA ELECTRÓNICA

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TITULO EN INGENIERÍA ELECTRÓNICA

"REINGENIERÍA Y OPTIMIZACIÓN DE LA RED DE VOZ Y DATOS DE PETROCOMERCIAL – REGIONAL NORTE"

ALEX HOMERO RIVADENEIRA ERAZO

SANGOLQUI – ECUADOR

MAYO – 2005

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado "REINGENIERIA Y OPTIMIZACION DE LA RED DE VOZ Y DATOS DE PETROCOMERCIAL – REGIONAL NORTE" ha sido desarrollado en su totalidad por el Sr. Alex Homero Rivadeneira Erazo.

Atentamente

Ing. Diego Balseca
DIRECTOR

Ing. Fabián Sáenz
CODIRECTOR

AGRADECIMIENTO

"En primer lugar te doy gracias Dios porque nunca me has abandonado y una vez más lo estás demostrando. Gracias Mami porque siempre has estado en los momentos más difíciles y me has ayudado a levantar, para continuar con mas fuerzas; gracias Papi por el ejemplo que me das y por todo lo que nos enseñaste de niños, gracias Jhoannita por tu compresión y apoyo, gracias Byron por todo lo nuevo que me has enseñado. En fin gracias y perdón familia por todo el sacrificio que han hecho por mi.

Y como olvidarme de mi tía Miche, gracias tía, porque si no hubiera sido por su apoyo en un inicio, yo no estaría aquí. Gracias señora Marthita por haberme tenido paciencia y por las bondades de su residencia, gracias Ing. Balseca, Ing. Vásconez, Ing. Sáenz y a todas las personas de Petrocomercial por el apoyo y paciencia que me brindaron para realizar este proyecto, gracias a toda mi familia y amigos que creen en mi, gracias a los buenos y malos profesores que me instruyeron y gracias a esta Institución."

Alex Rivadeneira

DEDICATORIA

Dedico este trabajo y todo el esfuerzo a lo largo de mi vida estudiantil con todo mi corazón a mi Mami, a mi Papi y a mis queridos Hermanos.

PRÓLOGO

El presente proyecto tiene por objetivo mejorar el desempeño de las principales redes locales de la Regional Norte de PETROCOMERCIAL, por medio del rediseño de estas redes y el diseño de redes de área local virtuales (VLANs), en base a las circunstancias, necesidades y disponibilidad de equipos de la empresa.

A través de los objetivos planteados, se consigue que las redes locales seleccionadas, obtengan flexibilidad y escalabilidad a través de una fácil administración, y además la factibilidad de seguridad en estas redes. También se mejora la calidad de voz sobre IP, debido a que a éste tráfico se le asigna su propia red virtual y una prioridad superior con respecto al tráfico de datos.

Todos los cambios que implica el diseño de VLANs y rediseño de la red como tal, es transparente para los usuarios, pero si son ellos los principales favorecidos porque ganan una mejor calidad de voz en las llamadas telefónicas sobre los teléfonos IP y una confiable y rápida comunicación con las diferentes aplicaciones de los servidores al igual que en la transferencia de archivos; además tienen un mejor servicio por parte de la administración de red, cuando se necesite mover o cambiar una estación de trabajo manteniendo los anteriores beneficios, y así mismo reciben una rápida solución a los problemas que se puedan presentar en la red.

Este proyecto sirve como modelo para realizar el diseño y configuración de VLANs de cualquier red local de Petrocomercial, si la empresa así lo requiere y las circunstancias futuras lo ameritan.

ÍNDICE

Pág.

CAPITULO I

ESTUDIO ACTUAL DE LA RED

1.1 INTRODUCCIÓN

La REGIONAL NORTE DE PETROCOMERCIAL está formada por varias redes de área local (LANs – *Local Area Networks*) ubicadas en La Matriz (Quito), terminales: Beaterio (Quito), Santo Domingo, Ambato, Shushufindi, Esmeraldas, entre otros; integradas a través de una red de área extendida (WAN – *Wide Area Network*).

A continuación se va a realizar un estudio detallado de cada una de las redes locales y de la red de área extendida, recopilando la información que se considera necesaria para conseguir los objetivos propuestos.

1.2 RED WAN DE LA REGIONAL NORTE

La red WAN de la Regional Norte de Petrocomercial, hace uso del protocolo de encapsulación *Frame Relay*, la cual se encuentra integrada por Routers Motorota, modelo Vanguard, y series: 6455, 6435 y 340; utilizando radio enlaces como medios de comunicación. De manera general la topología de la red WAN es una topología en estrella extendida, como se muestra en la Figura 1.1 y en la Figura 1.2, porque todos los terminales convergen en los dos routers del Pichincha, y se extienden a los lugares más lejanos a través de routers de intersección como el de Esmeraldas Pco (600), Condijua Pco (800) y Pin Shushufindi (820). Mientras que para llegar a Riobamba se utiliza un canal de 64Kbps por medio del proveedor de servicios Adinadatos.

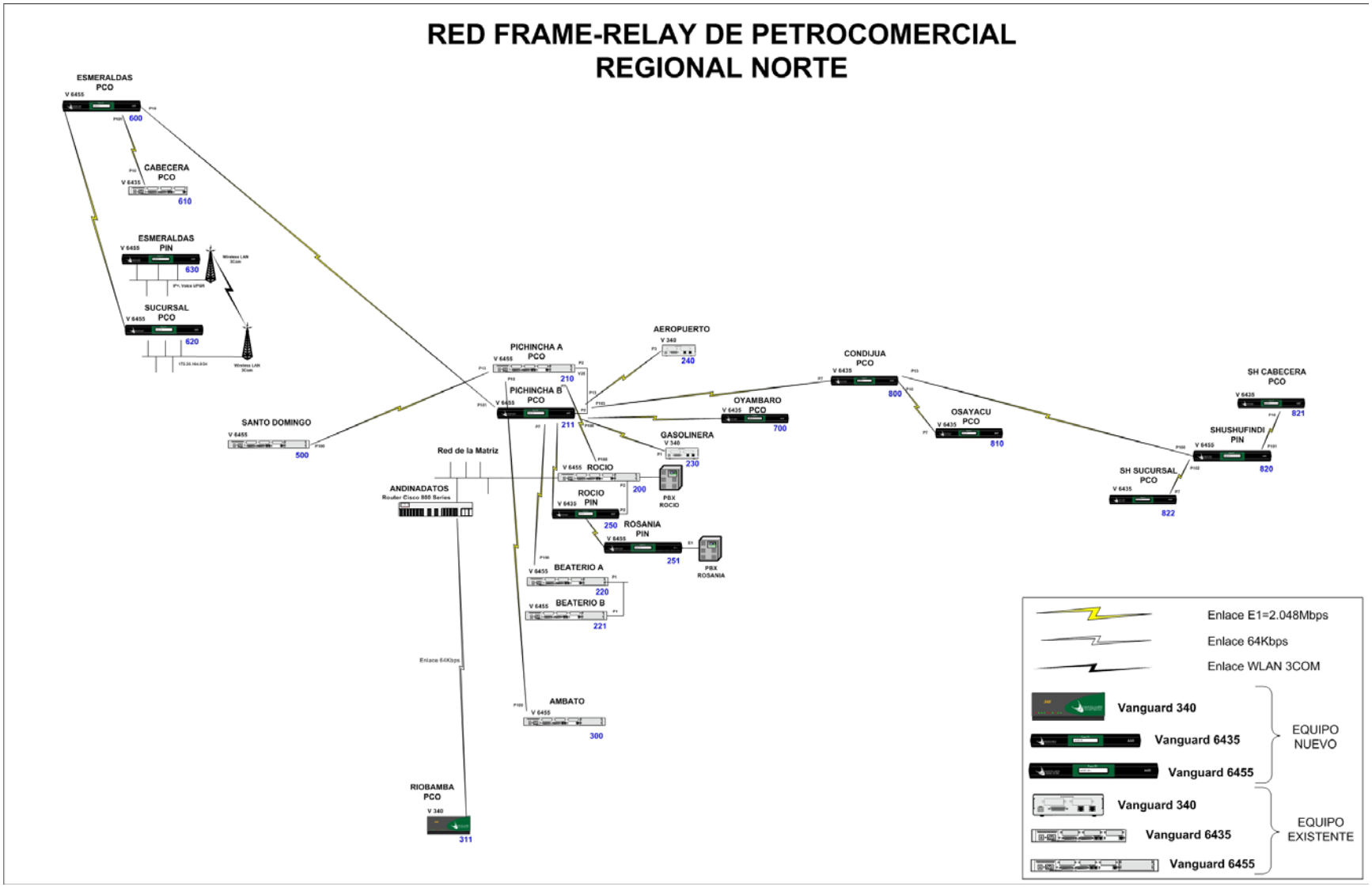


Figura 1.1 Red Frame Relay de Petrocomercial Regional Norte

1.2.1 Subneteo e Interfaces de la Red WAN

Cada una de las filiales de Petroecuador tiene asignada una dirección de red diferente, en este caso para la red de Petrocomercial, tanto la Regional Norte como la Regional Sur, es la dirección: 172.20.0.0, es decir es una red clase B; y a su vez esta red esta divida en sub-redes (subneteada), de tal forma que cada red local tiene asignada una dirección de subred diferente al igual que cada par de interfaces seriales que están enlazadas, así se muestra en la siguiente tabla:

INTERFACES DE LA RED WAN DE PETROCOMERCIAL - REGIONAL NORTE				
TERMINAL	**NODO**	**IP LAN**	**IP WAN desde EL ROCIO**	**IP WAN REMOTO**
Rocio	200	172.20.64.11/21		
Pichincha A	210		172.20.36.1/30	172.20.36.2/30
Pichincha B	211		172.20.40.125/27	172.20.40.126/27
Beaterio A	220	172.20.129.11/24	172.20.36.13/30	172.20.36.14/30
Beaterio B	221	172.20.129.12/24	172.20.36.29/30	172.20.36.30/30
Gasolinera	230	172.20.134.11/24	172.20.36.17/24	172.20.36.18/24
Aeropuerto	240	172.20.75.11/24	172.20.36.21/24	172.20.36.22/24
Pin Rocio	250			
Pin Rosanía	251	**172.17.16.23/24**		
Ambato	300	172.20.130.11/24	172.20.36.5/30	172.20.36.6/30
Riobamba	311	172.20.131.11/24	172.20.97.131/24	172.20.39.34/30
Sto. Domingo	500	172.20.161.11/24	172.20.36.9/30	172.20.36.10/30
Sucursal Sto. Dom.	-	172.20.162.11/24	172.20.32.94/30	172.20.32.93/30
Pco. Esmeraldas	600		172.20.36.129/30	172.20.36.130/30
Cabecera Esm.	610	172.20.163.11/24	172.20.36.133/30	172.20.36.134/30
Sucursal Esm.	620	172.20.164.11/24	172.20.36.137/30	172.20.36.138/30
Pin. Esmeraldas	630	**172.17.20.22/24**	172.20.36.141/30	172.20.36.142/30
Oyambaro	700	172.20.76.10/24	172.20.36.169/30	172.20.36.170/30
Condijua	800		172.20.36.153/30	172.20.36.154/30
Osayacu	810	172.20.136.10/24	172.20.36.157/30	172.20.36.158/30
Pin Shushufindi	820	**172.17.24.22/22**	172.20.36.149/30	172.20.36.150/30
Cabecera Shush.	821	172.20.137.11/24	172.20.36.161/30	172.20.36.162/30
Sucursal Shush.	822	172.20.138.11/24	172.20.36.165/30	172.20.36.166/30
Rocio-Terminales	-		172.20.64.11/21	172.20.64.2/21
Corazón	-	172.20.77.10/24	172.20.32.5/30	172.20.32.6/30
Chalpi	-	172.20.139.10/24	172.20.32.13/30	172.20.32.14/30
Quijos	-	172.20.140.10/24	172.20.32.17/30	172.20.32.18/30

Tabla 1.1 Interfaces de la Red WAN de Petrocomercial – Regional Norte

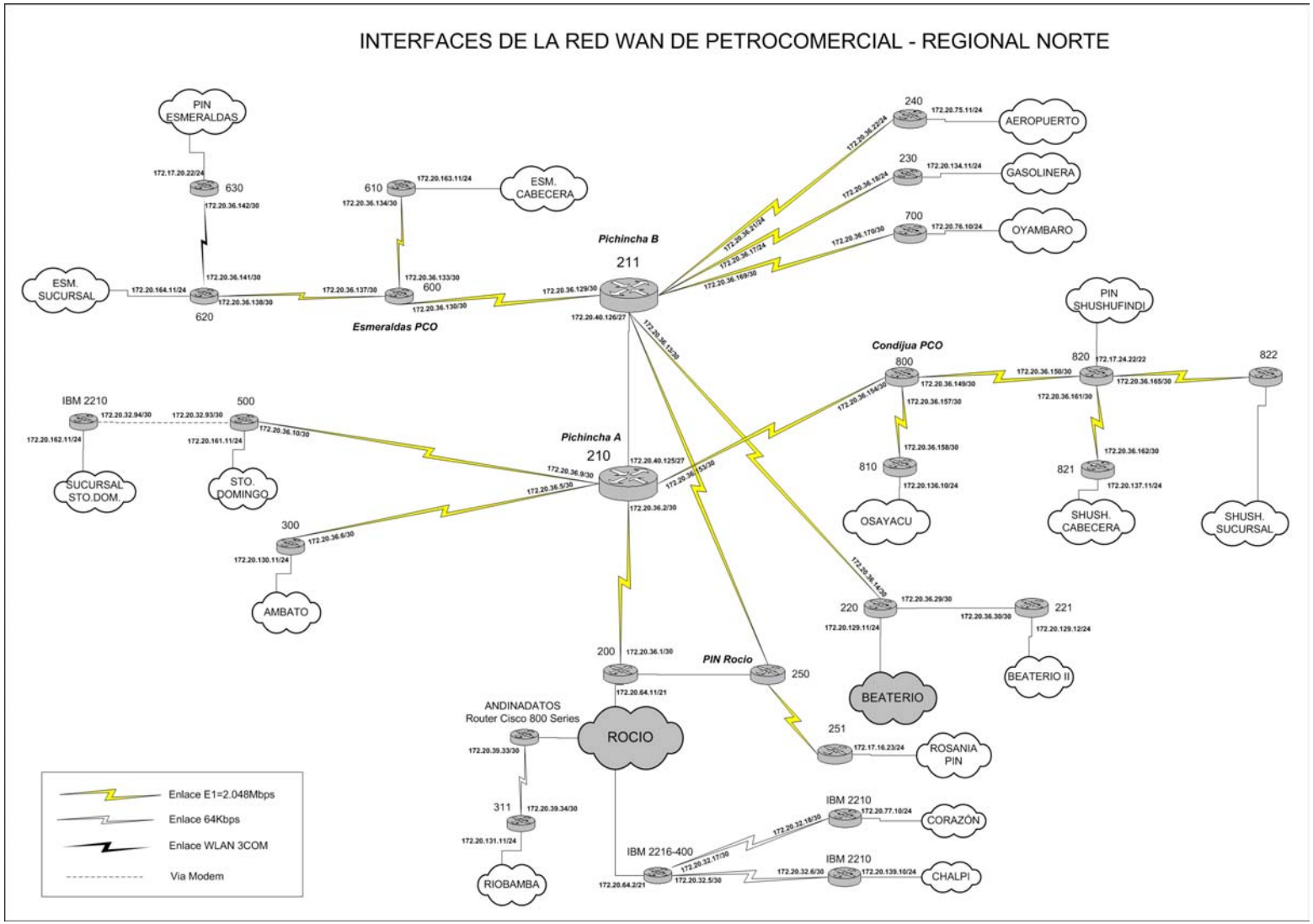


Figura 1.2 Interfaces de la Red WAN de Petrocomercial – Regional Norte

También forman parte de la red WAN Regional Norte, los terminales: Corazón, Chalpi, y próximamente Quijos, pero con el protocolo de encapsulación *Point to Point (PPP)*, empleando routers IBM 2210, modems y multiplexores - demultiplexores Bayly por medio de canales o enlaces de 64Kbps. Mientras que para llegar a la Sucursal Sto. Domingo se lo realiza utilizando modems, e igualmente con un router IBM 2210.

El levantamiento de esta información se la realizó de la siguiente forma:

Se ingresa vía telnet a cada uno de los routers Vanguard, apuntando a la dirección IP de una de las interfaces correspondientes al router que deseo conectarme.

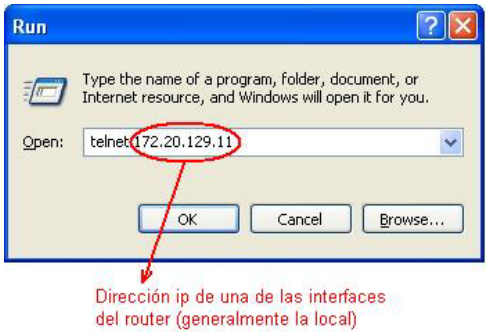


Figura 1.3 Ingreso a un Router Vanguard Vía Telnet

Luego, se digita el comando: "atds", que sirve para ingresar al router directamente.

Figura 1.4 Ingreso a un Router Vanguard Directamiente

Pero en el caso de no conocer la dirección IP de ninguna de las interfaces del router deseado, entonces se puede ingresar haciendo primero telnet a la interfaz de cualquier otro router dentro de la WAN Frame Relay, y luego digitar "atdp"+"#nodo frame relay"+"98", como se muestra en la Figura 1.5

Nota: Estos routers tienen asignados una identificación dentro de la nube Frame Relay, que se denomina el número de nodo.

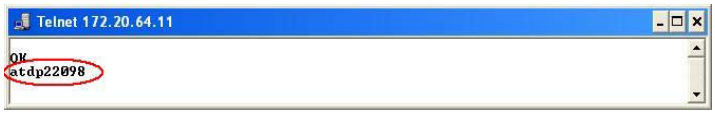


Figura 1.5 Ingreso a un Router Vanguard Indirectamente

Después de escribir la respectiva clave del router, se presenta a continuación el menú principal del mismo, tal como se muestra en la Figura 1.6.

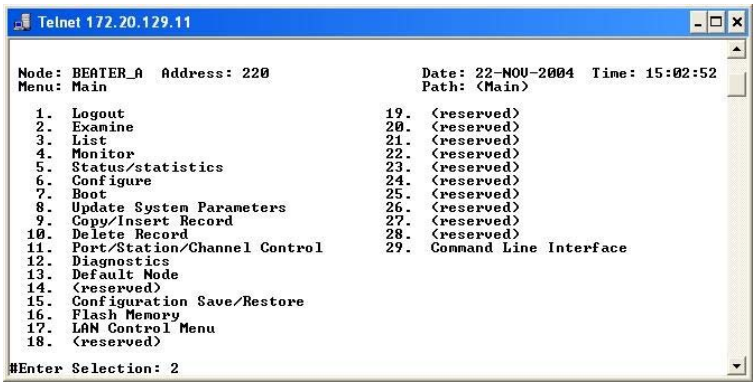


Figura 1.6 Menú Principal del Router Vanguard

Para conocer las interfaces que maneja cada router se debe elegir la siguiente secuencia de opciones: **Examine -> Examine Router -> Examine IP -> Interfaces**, y obtenemos la dirección IP que esta utilizando cada una de las interfaces con su respectiva máscara.

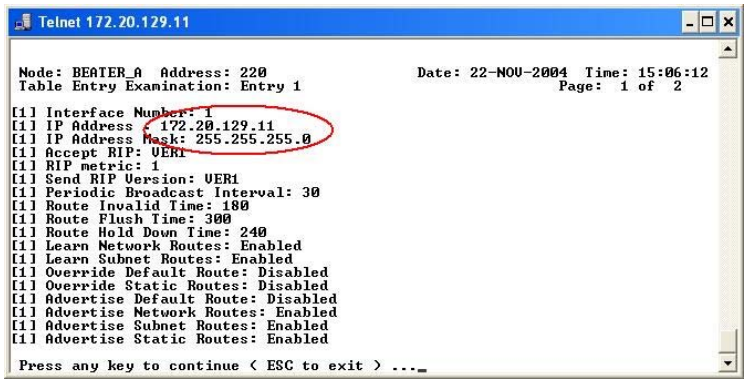


Figura 1.7 Dirección IP y Máscara de las Interfaces de un Router Vanguard

Toda esta información es elemental, para saber como ingresar a cada uno de los nodos y conocer como se encuentran las direcciones IP repartidas en cada una de las redes locales, y así poder configurar los routers cuando llegue a ser necesario. Razón por la cual también se presenta un resumen detallado de los routers que se están utilizando en cada uno de los nodos, con la versión de su respectivo sistema operativo (IOS), porque de ello dependerá si soportan o no los protocolos y configuraciones que habrá que realizar.

ROUTERS DE LA REGIONAL NORTE			
Lugar	**Router**	**Nodo**	**Versión IOS**
Rocio	Motorola Vanguard 6455	200	V6.4.S10A
Pichincha A	Motorola Vanguard 6455	210	V6.4.S10A
Pichincha B	Motorola Vanguard 6455	211	V6.4.S10A
Beaterio A	Motorola Vanguard 6455	220	V6.4.S10A
Beaterio B	Motorola Vanguard 6455	221	V6.4.S10A
Gasolinera	Motorola Vanguard 340	230	V5.6.R000
Aeropuerto	Motorola Vanguard 340	240	V5.6.R000
Pin Rocio	Motorola Vanguard 6435	250	V6.4.S10A
Pin Rosanía	Motorola Vanguard 6455	251	V6.1.R000
Ambato	Motorola Vanguard 6455	300	V5.6.R000
Riobamba	Motorola Vanguard 340	311	V6.0.R00A
Sto. Domingo	Motorola Vanguard 6455	500	V6.1.R000
Sucursal Sto. Dom.	IBM 2210	-	-
Pco. Esmeraldas	Motorola Vanguard 6455	600	V6.1.R000
Cabecera Esm.	Motorola Vanguard 6435	610	V6.0.S100
Sucursal Esm.	Motorola Vanguard 6455	620	V6.1.T14A
Pin. Esmeraldas	Motorola Vanguard 6455	630	V6.1.R000
Oyambaro	Motorola Vanguard 6435	700	V6.2.R000
Condijua	Motorola Vanguard 6435	800	V6.0.S100
Osayacu	Motorola Vanguard 6435	810	V6.0.S100
Pin Shushufindi	Motorola Vanguard 6455	820	V6.1.R000
Cabecera Shush.	Motorola Vanguard 6435	821	V6.1.R000
Sucursal Shush.	Motorola Vanguard 6435	822	V6.0.S100
Rocio-Terminales	IBM 2216-400	-	V3.1
Corazón	IBM 2210	-	V3.3
Chalpi	IBM 2210	-	V3.2
Quijos	IBM 2210	Planificado	

Tabla 1.2 Versión del IOS de los Routers de Petrocomercial - Regional Norte

Para recuperar la serie del router y versión del sistema operativo que está utilizando, se ingresa a **Statistics -> Node.** Ver Figura 1.8

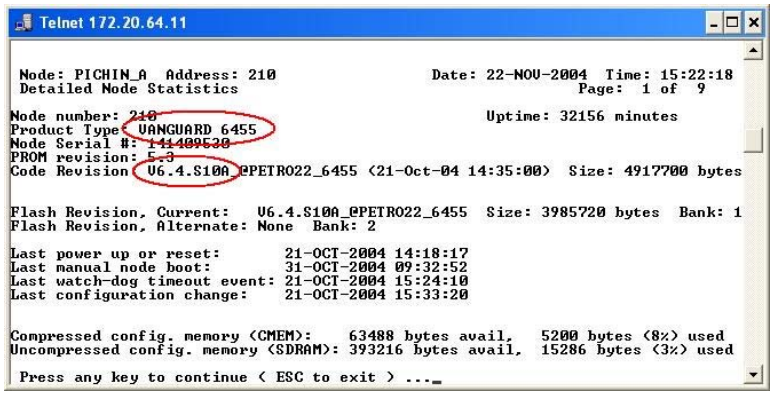


Figura 1.8 Serie y Versión del Router Vanguard

1.2.2 Red Nacional de Teleproceso

En la Figura 1.9 se distingue principalmente la ubicación de:

- Los servidores (ver detalle en Anexo 1), los accesos a: las sucursales (Cuenca, Riobamba, Guayaquil-*backup*), los terminales (Corazón, Chalpi), la red WAN y el acceso remoto *Dial-up*, además de la intranet de la Matriz. Todos estos forman parte de la VLAN[1] 1.
- Lo que constituye la red externa, con el servidor Web, y los accesos a: Internet, al SRI, al Ministerio de Energía y Minas (DNH) que forman parte de la VLAN 2.
- Los accesos a las filiales como: Petroecuador, SOTE y Petroproducción que están en la VLAN 3.

Estas tres VLANs están definidas sobre el switch Cisco Catalyst 3500 XL (Pco_155) con etiqueta SW155C (detalle de puertos en Anexo 2); separadas y protegidas con el Firewall AIX IBM (ver Anexo 1).

Además se encuentran los Servidores I-Series (AS/400) con las etiquetas PCO1, PCO2, PCO8/PCO9, que se utilizan en diferentes aplicaciones en la red de Petrocomercial (ver detalles en Anexo 1), así como la Central Telefónica IP Mitel que da servicio a la red de La Matriz y a otras terminales. Tanto los enlaces a Guayaquil, Galápagos y Cuenca son responsabilidad de la Regional Sur de Petrocomercial; así como todos los enlaces E1 que se desprenden de Cerro Azul.

[1] Virtual Local Area Network

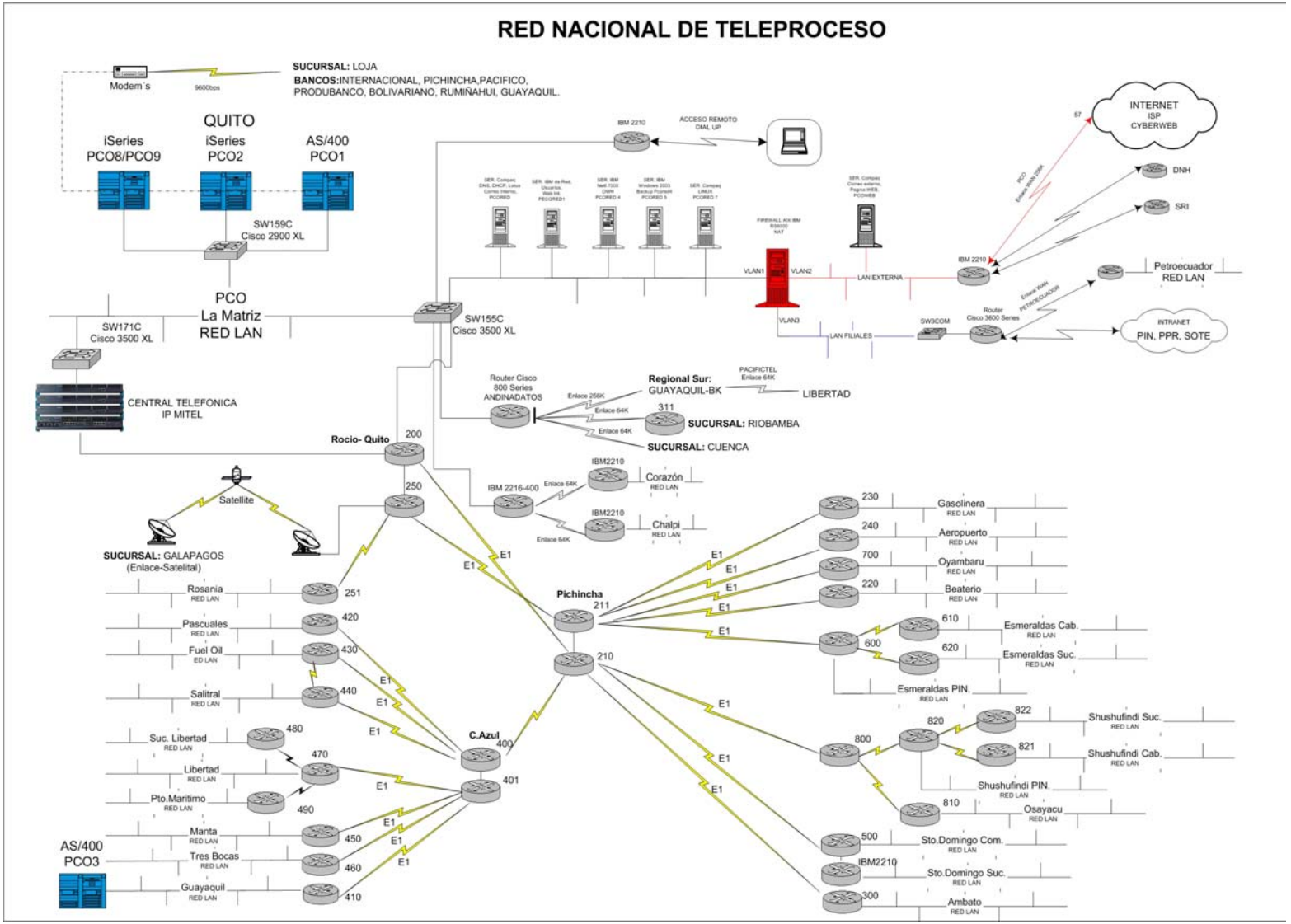


Figura 1.9 Red Nacional de Teleproceso de Petrocomercial

1.2.3 Jerarquía de Departamentos de Petrocomercial

La presente información es importante porque aquí se detalla como están agrupados y organizados cada uno de los departamentos en forma administrativa, sin importar su ubicación física, lo cual será una gran ayuda el momento de diseñar la distribución de VLANs en toda la red.

JERARQUIA DE DEPARTAMENTOS DE PETROCOMERCIAL	
CONTRALORIA GENERAL DEL ESTADO	CTR
CAJITA DE PCO	CPECO
FONDO DE JUBILACION	
VICEPRESIDENCIA (Asesores de Vicepresidencia)	VCP
LEGAL VICEPRESIDENCIA (Asesoria Legal)	VLE
PLANIFICACION Y FINANZAS	VPF
PROGRAMACION	VPR
RELACIONES PUBLICAS	VRP
CONTROL DE GESTION	VCG
GERENCIA REGIONAL NORTE	VGN
COORDINACION DE CONTRATOS	GCC
CONTROL DE GESTION	GCG
PROTECCION AMBIENTAL Y SEGURIDAD INDUSTRIAL	GPI
PROTECCION AMBIENTAL	IPA
SEGURIDAD INDUSTRIAL	ISI
LEGAL GERENCIA NORTE	GLE
ASESORIAS	LAS
PROCESOS	LPR
PROYECTOS	GPR
EJECUCION DE PROYECTOS	PEP
EVALUACION DE PROYECTOS	PEV
REAJUSTE DE PRECIOS	PRP
SISTEMAS Y TELECOMUNICACIONES	GSI
INGENIERIA Y PROCESAMIENTO	SIP
REDES Y TELECOMUNICACIONES	SRT
SOPORTE Y APLICACIONES	SSA
SOPORTE TECNICO Y MANTENIMIENTO	SST
SUBGERENCIA DE ADMINISTRACION Y FINANZAS	GSA
ADMINISTRATIVA	AAD
BIENESTAR LABORAL	DBL
RECURSOS HUMANOS	DRH
SERVICIOS ADMINISTRATIVOS	DSA
SEGURIDAD FISICA	DSF
SECRETARIA GENERAL	DSG
FINANZAS	AFI
ADMINISTRACION DE ACTIVOS	FAA
ADMINISTRACION FINANCIERA	FAF
CREDITO Y COBRANZAS	FCC
CONTABILIDAD	FCO
PRESUPUESTO	FPR
SEGUROS Y GARANTIAS	FSG
CUENTAS POR PAGAR	FCP
MATERIALES	AMA
COMPRAS LOCALES	MCL
IMPORTACIONES	MIM
CONTROL DE MATERIALES Y BODEGAS	MCM
BODEGA DE BEATERIO	MBB
BODEGA DE OSAYACU	MBO
BODEGA DE STO. DOMINGO	MBS

SUBGERENCIA DE COMERCIALIZACION	GSC
ABASTECEDORA	CAB
FACTURAS Y VENTAS	BFV
LIQUIDACION Y CONSOLIDACION DE CUENTAS	BLC
COORDINACION OPERATIVA	BCO
SUCURSAL AMBATO	BSA
SUCURSAL ESMERALDAS	BSE
SUCURSAL SHUSHUFINDI	BSH
SUCURSAL QUITO	BSQ
SUCURSAL RIOBAMBA	BSR
SUCURSAL STO. DOMINGO	BSS
COMERCIALIZADORA	CKO
ADMINISTRACION DE NEGOCIOS PROPIOS	KAN
COORDINACION OPERATIVA DE VENTAS	KCO
MERCADEO Y ATENCION AL CLIENTE	KMA
SUBGERENCIA DE TRANSPORTE Y ALMACENAMIENTO	GST
MOPRO	TMP
INSPECCION TECNICA	TIT
CONTROL DE CALIDAD	TCC
SUPERINTENDENCIA POLIDUCTO ESM-STO.DMGO-QUITO-MAC.	TPE
MANTENIMIENTO ELECTROMECANICO E-SD-Q-M	EME
MANTENIMIENTO DE LINEA E-SD-Q-M	EML
OPERACIONES E-SD-Q-M	EOP
ESTACION REDUCTORA BEATERIO	EEB
ESTACION DE BOMBEO CORAZON	EEC
ESTACION CABECERA ESMERALDAS	EEE
ESTACION DE BOMBEO FAISANES	EEF
ESTACION DE BOMBEO STO. DOMINGO	EES
INSPECCION TECNICA POL. E-SD-Q-M	EIT
SUPERINTENDENCIA POLIDUCTO QUITO-AMBATO-RIOBAMBA	TPQ
MANTENIMIENTO ELECTROMECANICO QUITO-AMBATO-RIOBAMBA	QME
MANTENIMIENTO DE LINEA QUITO-AMBATO-RIOBAMBA	QML
OPERACIONES QUITO-AMBATO-RIOBAMBA	QOP
ESTACION AMBATO	QEA
INSPECCION TECNICA POL. QUITO-AMBATO-RIOBAMBA	QIT
SUPERINTENDENCIA POLIDUCTO SHUSHUFINDI - QUITO	TPH
MANTENIMIENTO ELECTROMECANICO SHUSHUFINDI - QUITO	HME
MANTENIMIENTO DE LINEA SHUSHUFINDI - QUITO	HML
OPERACIONES SHUSHUFINDI - QUITO	HOP
ESTACION CHALPI	HEC
ESTACION SHUSHUFINDI	HEH
ESTACION OSAYACU	HEO
ESTACION QUIJOS	HEQ
INSPECCION TECNICA POL. SHUSHUFINDI - QUITO	HIT
SUPERINTENDENCIA TERMINALES Y DEPOSITOS	TYD
TERMINALES Y DEPOSITOS	YTD
CONTROL DE CALIDAD TERMINALES Y DEPOSITOS	YCC
DESPACHO DE TERMINALES Y DEPOSITOS	YDE
DEPOSITO RIOBAMBA	YDR
INSPECCION TECNICA TERMINALES Y DEPOSITOS	YIT
MOPRO TERMINALES Y DEPOSITOS	YMP
MANTENIMIENTO TERMINALES Y DEPOSITOS	YMT
TERMINAL AMBATO	YTA
TERMINAL PRODUCTOS LIMPIOS BEATERIO	YTB
TERMINAL STO. DOMINGO	YTS
ALMACENAMIENTO Y DESPACHO PLANTA DE GAS OYAMBARO	YAG
PLANTA DE GAS OYAMBARO	YGO
MOPRO PLANTA DE GAS OYAMBARO	YMG

Tabla 1.3 Jerarquía de Departamentos de Petrocomercial

1.3 RED DE LA MATRIZ

La red local ubicada en la Matriz-Quito, conformada por los edificios: El Rocio y Ex-Salesianos, es la más grande e importante de todas, porque aquí se centraliza la administración de la empresa, así como el control y mantenimiento de los servidores e I-Series (AS/400), cuyas aplicaciones son utilizadas a nivel nacional.

1.3.1 Topología Básica de la Red La Matriz

La actual red de los edificios El Rocio y Ex-Salesianos, está formado por un backbone de fibra óptica multimodo, con una topología tipo bus y enlaces de cable UTP de 100 Mbps a los switches más alejados y a los servidores de red, como se muestra en la Figura 1.10.

Los principales accesos son a Internet, al SRI, al Ministerio de Energía y Minas (DNH), a las filiales como Petroecuador, Petroindustrial, SOTE, Petroproducción; a Sucursales como: Riobamba, Cuenca y Guayaquil; a Terminales como: Corazón y Chalpi; y necesariamente a la red WAN de PETROCOMERCIAL.

Además la red actual de La Matriz está formada por cuatro *clusters*, que ayudan a conseguir un mejor control y administración de la red, a través del programa **"*Cluster Managment Suite*"**, para Switches Cisco Catalyst. Este programa permite manejar simultáneamente hasta 16 switches dispersos geográficamente con una sola dirección IP, el acceso es vía *web browser*, provee interfaces gráficas para configuración y administración de los elementos Cisco; y soporta los siguientes elementos Catalyst: 1900/2820, 2900 XL, 3500 XL, 2950 y 3550.

Los servidores se encuentran conectados con cable UTP a 100 Mbps al cluster 1, tanto al switch Pco_151 como al switch Pco_159. Ver Figura 1.10.

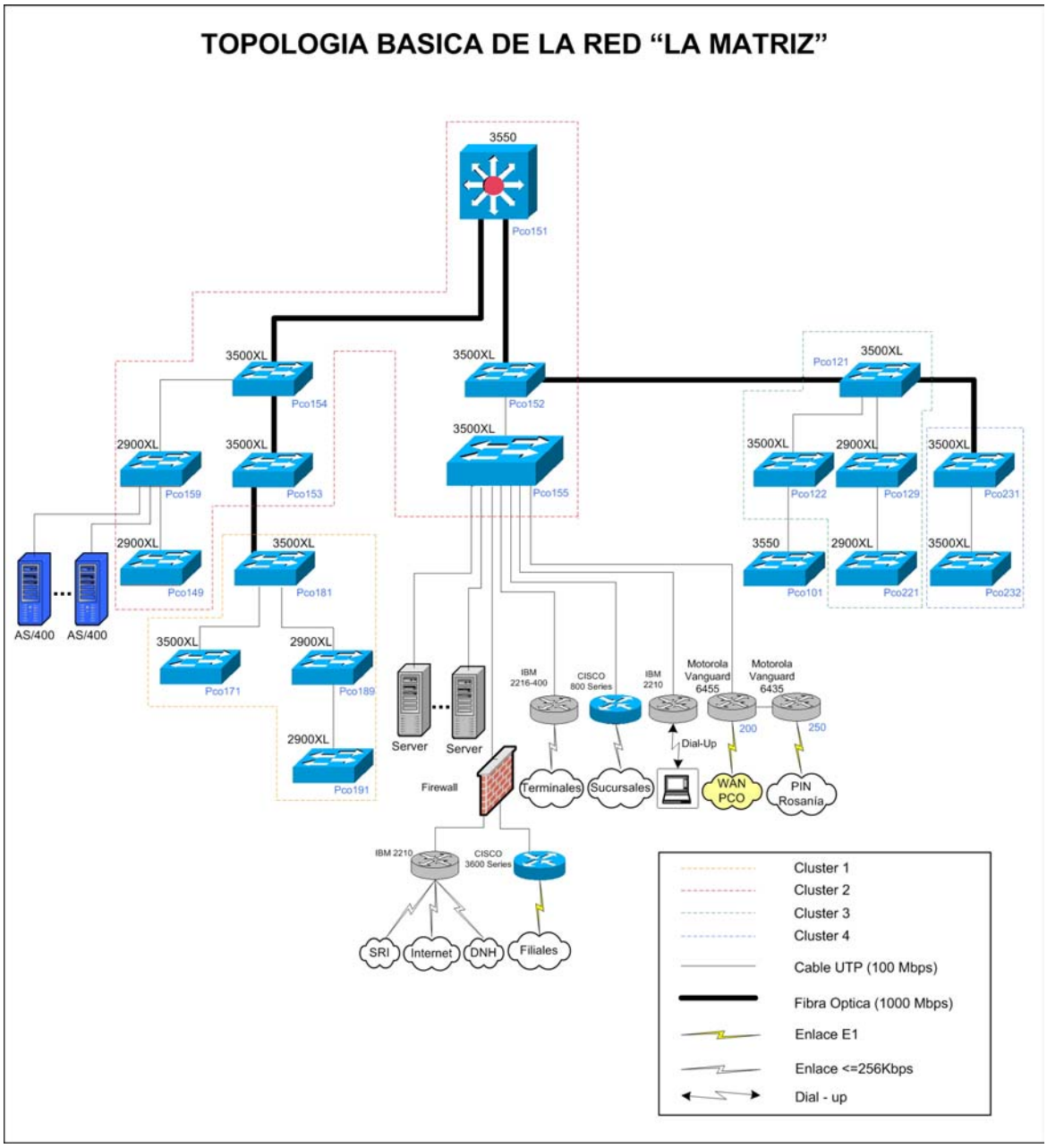


Figura 1.10 Topología Básica de la Red de la Matriz

1.3.2 Interconexión de los Elementos Activos de Red de la Matriz

Es importante determinar la interconexión de los dispositivos de red, (en los edificios de El Rocio y Ex-Salesianos), para saber que medios, interfaces y equipos se están utilizando, es decir para conocer como esta dispuesta la red actual de la Matriz, y así ayudar a la determinación de cambios que sean necesarios en el nuevo rediseño de esta red.

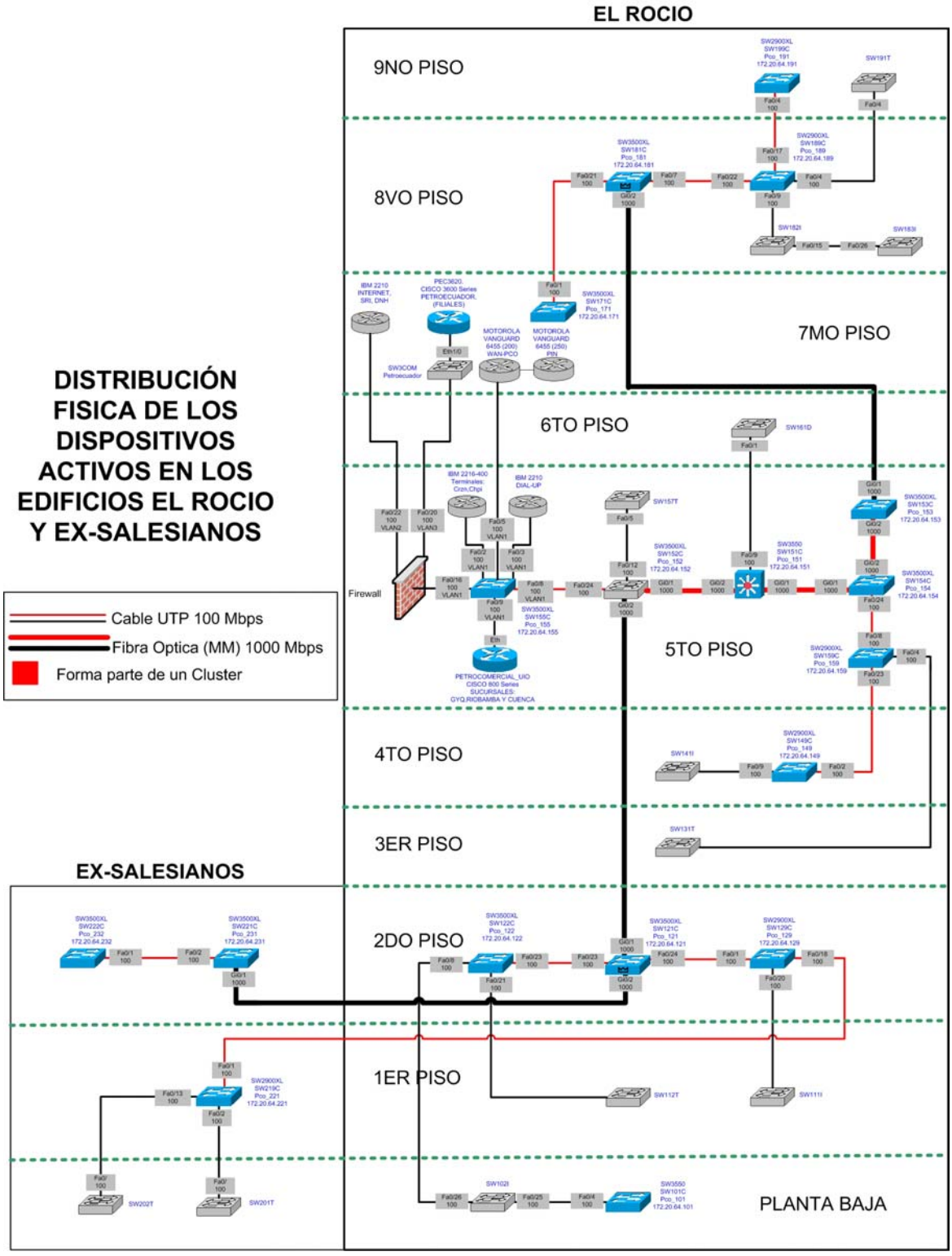


Figura 1.11 Distribución Física de los Dispositivos Activos en la Red de la Matriz

Para obtener parte de esta información se utilizó el programa *Cluster Managment Suite*, antes mencionado, que permite ver de forma gráfica la topología de cada cluster (ver Figura 1.12), la velocidad a la que están conectados, los nombres de los equipos, sus

direcciones IP, e incluso sus direcciones MAC. Además se verificó esta información vía telnet utilizando el comando "**show cdp neighbors"**, en cada uno de los switches Cisco.

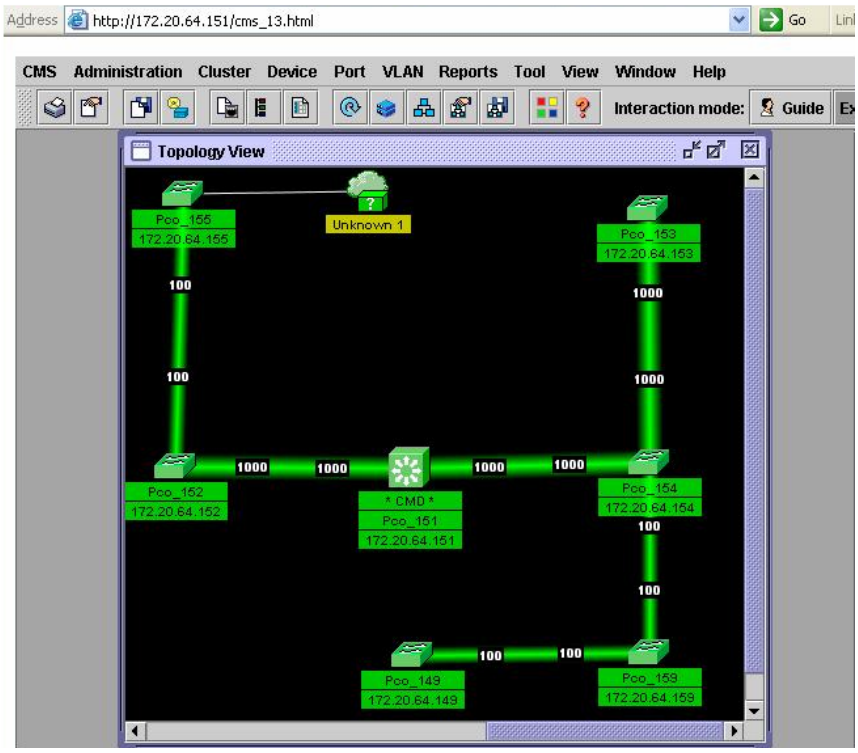


Figura 1.12 Cluster Managment Suite

Mientras que para localizar los switches IBM, 3COM y otros, se realizó una inspección personal, que además ayudo a reconocer la ubicación física de todos los elementos activos de red.

Cada uno de los *clusters* se encuentra comandado por:

- Pco_121 en Cluster 1
- Pco_151 en Cluster 2
- Pco_181 en Cluster 3
- Pco_232 en Cluster 4

En resumen los switches Cisco que integran cada uno de los cuatro clusters que existen en la red de La Matriz son:

SWITCHES CISCO DE "LA MATRIZ"							
Cluster	**Nombre**	**Dirección IP**	**Etiqueta**	**Switch**	**Modelo**	**Version IOS**	**Dirección MAC**
Cluster 1	Pco_171	172.20.64.171	SW171C	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	00:0A:8A:39:E4:40
	Pco_181	172.20.64.181	SW181C	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	00:0A:8A:5B:4E:C0
	Pco_189	172.20.64.189	SW189C	Cisco Catalyst 2900 XL Series	WS-C2924-XL-EN	12.0 (5.2) XU	00:04:C1:F5:66:C0
	Pco_191	172.20.64.191	SW199C	Cisco Catalyst 2900 XL Series	WS-C2912-XL-EN	12.0 (5.2) XU	00:04:C0:9F:10:00
Cluster 2	Pco_149	172.20.64.149	SW149C	Cisco Catalyst 2900 XL Series	WS-C2912-XL-EN	12.0 (5.2) XU	00:04:C1:AA:26:40
	Pco_151	172.20.64.151	SW151C	Cisco Catalyst 3550 Series	WS-3550-24-PWR-SMI	12.1 (13) EA1a	00:0D:BD:B2:87:80
	Pco_152	172.20.64.152	SW152C	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	00:0A:41:B4:61:40
	Pco_153	172.20.64.153	SW153C	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	00:0A:8A:5B:60:C0
	Pco_154	172.20.64.154	SW154C	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	00:0A:8A:39:B2:40
	Pco_155	172.20.64.155	SW155C	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	00:0A:F4:F2:C8:C0
	Pco_159	172.20.64.159	SW159C	Cisco Catalyst 2900 XL Series	WS-C2924-XL-EN	12.0 (5.2) XU	00:04:C1:F5:8F:00
Cluster 3	Pco_121	172.20.64.121	SW121C	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	00:0A:8A:39:CC:40
	Pco_122	172.20.64.122	SW122C	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	00:0A:8A:3A:3E:00
	Pco_129	172.20.64.129	SW129C	Cisco Catalyst 2900 XL Series	WS-C2924-XL-EN	12.0 (5.2) XU	00:04:C1:F5:88:00
	Pco_221	172.20.64.221	SW219C	Cisco Catalyst 2900 XL Series	WS-C2924-XL-EN	12.0 (5.2) XU	00:04:C1:DE:80:00
Cluster 4	Pco_231	172.20.64.231	SW221C	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	00:0A:F4:F2:C6:40
	Pco_232	172.20.64.232	SW222C	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	00:0A:8A:4C:CB:C0
Indpte.	Pco_101	172.20.64.101	SW101C	Cisco Catalyst 3550 Series	WS-3550-24-PWR-SMI	12.1 (14) EA1a	00:0F:24:EA:10:80

Tabla 1.4 Switches Cisco de la Matriz

El resto de switches que no son Cisco y no forman parte de los clusters pero que igual son parte de la red La Matriz, son:

Switches: IBM, 3COM y Dlink de La Matriz			
Etiqueta	**Switch**	**Modelo**	**Dirección MAC**
SW102I	IBM 10/100	8271-E24	00:90:04:EC:54:F8
SW111I	IBM 10/100	8271-E24	00:90:04:37:FE:F8
SW141I	IBM 10/100	8275-217	00:90:AC:D9:09:C5/C4
SW182I	IBM 10/100	8271-E24	00:90:04:EC:51:78
SW183I	IBM 10/100	8271-E24	00:90:04:EC:53:F8
SW112T	3COM 10/100	8 puertos	
SW131T	3COM 10/100	8 puertos	
SW157T	3COM 10/100	5 puertos	
SW191T	3COM 10/100	8 puertos	
SW201T	3COM 10/100	8 puertos	
SW202T	3COM 10/100	8 puertos	
SW161D	DLINK 10/100	8 puertos	

Tabla 1.5 Switches IBM, 3COM y Dlink de la Matriz

Es decir existen: 2 Switches Cisco 3550, 10 Swtiches Cisco 3500 XL, 6 Switches Cisco 2900 XL, 5 Switches IBM, 6 Switches 3COM y 1 Switch DLINK. Los routers que se están utilizando para proveer los diferentes accesos son:

Routers de acceso de La Matriz	
Router	**Acceso a:**
Motorola Vanguard 6455	WAN de Petrocomercial
Motorola Vanguard 6435	Petroindustrial
Cisco 3600 Series	Filiales: Petroecuador, SOTE, Petroproducción
Cisco 800 Series	Sucursales: Guayaquil, Riobamba y Cuenca
IBM 2216-400	Terminales: Corazón y Chalpi
IBM 2210	Internet, SRI, Ministerio de Energía y Minas
IBM 2210	PC vía Dial - up

Tabla 1.6 Routers de Acceso de la Matriz

1.3.3 Equipos de la Red La Matriz

Para desarrollar el rediseño de la red La Matriz a través de redes de área local virtuales, es necesario conocer la cantidad de equipos que maneja cada una de las unidades o departamentos, como se muestra en la siguiente tabla:

CANTIDAD DE ESTACIONES DE TRABAJO EN LA RED DE LA MATRIZ					
UNIDAD O DEPARTAMENTO	#PC's	#IMP	#TEL	#EQ	Ptos
CONTRALORIA GENERAL DEL ESTADO	5				5
CAJITA DE PCO	1				1
FONDO DE JUBILACION	6				6
VICEPRESIDENCIA (Asesores de Vicepresidencia)	9		3		12
LEGAL VICEPRESIDENCIA (Asesoria Legal)	3				3
PLANIFICACION Y FINANZAS	5				5
PROGRAMACION	6				6
RELACIONES PUBLICAS	2		1		3
CONTROL DE GESTION	7		3		10
GERENCIA REGIONAL NORTE	5				5
COORDINACION DE CONTRATOS	8	1			9
CONTROL DE GESTION	2				2
LEGAL GERENCIA NORTE	12	1	1		14
ASESORIAS	0				0
PROCESOS	4				4
PROYECTOS	3				3
EJECUCION DE PROYECTOS	7		1		8
EVALUACION DE PROYECTOS	4				4
REAJUSTE DE PRECIOS	0				0
SISTEMAS Y TELECOMUNICACIONES	4	4	2		10
INGENIERIA Y PROCESAMIENTO	6			15	21
REDES Y TELECOMUNICACIONES	4		2	7	13
SOPORTE Y APLICACIONES	19	1			20
SOPORTE TECNICO Y MANTENIMIENTO	7	1			8
SUBGERENCIA DE ADMINISTRACION Y FINANZAS	2				2
ADMINISTRATIVA	3				3
BIENESTAR LABORAL	2		2		4
RECURSOS HUMANOS	8				8
SERVICIOS ADMINISTRATIVOS	11	1	2		14
SEGURIDAD FISICA	3			1	4
SECRETARIA GENERAL	4		1		5
FINANZAS	2		1		3
ADMINISTRACION DE ACTIVOS	5				5
ADMINISTRACION FINANCIERA	10		2		12
CREDITO Y COBRANZAS	9		1		10
CONTABILIDAD	15	1			16
PRESUPUESTO	4	1	1		6
SEGUROS Y GARANTIAS	6				6
CUENTAS POR PAGAR	4				4
MATERIALES	2				2
COMPRAS LOCALES	5				5
IMPORTACIONES	5				5
CONTROL DE MATERIALES Y BODEGAS	5				5
SUBGERENCIA DE COMERCIALIZACION	2				2
ABASTECEDORA	2	2			4
FACTURAS Y VENTAS	6				6
LIQUIDACION Y CONSOLIDACION DE CUENTAS	4				4
COORDINACION OPERATIVA	5				5
COMERCIALIZADORA	6	1			7
ADMINISTRACION DE NEGOCIOS PROPIOS	2				2
COORDINACION OPERATIVA DE VENTAS	3				3
MERCADEO Y ATENCION AL CLIENTE	3				3
SUBGERENCIA DE TRANSPORTE Y ALMACENAMIENTO	8	1	2		11
CANTIDAD TOTAL DE HOSTS EN LA MATRIZ:	275	15	25	23	338

Tabla 1.7 Cantidad de Estaciones de Trabajo en la Matriz

Nota: El número de teléfonos que se muestra en la Tabla 1.7, es la cantidad de teléfonos IP independientes, es decir aquellos que no están conectados con una computadora.

En la siguiente tabla, se muestra un resumen de la cantidad de equipos que existe en la red La Matriz:

Equipos existentes en La Matriz	
Cant.	**Detalle:**
275	Computadoras
138	Teléfonos IP en la red "La Matriz"
15	Impresoras de red
1	Equipo DSR-2000 Califur by Kalatel (Para Seguridad Física)
1	Central Telefónica IP Mitel
1	Firewall (3 tarjetas de red)
8	Servidores (6 funcionan actualmente)
4	I-Series (AS/400)
7	Routers (El router Vanguard 6435 está conectado al Vanguard 6455)

Tabla 1.8 Equipos Existentes en la Matriz

Nota: Existen teléfonos IP que no están conectados a computadoras (pero ya están incluidos en la cantidad de teléfonos antes mencionada), y otros teléfonos IP que llegan hasta otros terminales, estos son:

Teléfonos IP independientes y remotos	
Cant.	**Detalle:**
25	Teléfonos IP independientes en la red "La Matriz"
8	Teléf. IP que llegan a terminales como Beaterio,Sto.Dom,Oyambaro y Osayacu

Tabla 1.9 Teléfonos IP Independientes y Remotos

Por lo tanto el número total de puntos de red necesarios en la Matriz, son:

Cantidad de puntos de red necesarios en La Matriz	
Cant.	**Puntos de red necesarios para:**
275	Computadoras
15	Impresoras de red
23	Equipos (Servidores,AS/400s, Firewall, Routers, Central IP, DSR-2000)
25	Teléfonos IP independientes
338	**NUMERO TOTAL DE PUNTOS DE RED EN LA MATRIZ**

Tabla 1.10 Cantidad de Puntos de Red necesarios en la Matriz

Toda esta importante información es el resumen de una gran base de datos (Anexo 3, Anexo 4 y Anexo 5) que se obtuvo de varias formas y que se describe a continuación:

Para el caso de las computadoras, se extrajo una base de datos del Servidor DHCP, en la que constaban las direcciones MAC de todas las computadoras, con su respectivo nombre de maquina, que tienen el formato: XYZNA, donde XYZ son las siglas que identifican al departamento, N es la inicial del primer nombre de la persona que usa la máquina y A es la inicial de su apellido paterno; y luego se comparo con las direcciones MAC que se obtenían de cada uno de los switches Cisco utilizando el comando **"show MAC-address".** Ver Anexo 3.

Para los teléfonos IP, en forma similar se obtuvo una base de datos en este caso de la Central Telefónica Mitel, que describía la extensión y la dirección MAC de los teléfonos, luego a estos se los compara con la guía telefónica del edificio y se encontraba a quien y a que departamento pertenece; y para saber a que switch estaban conectados, se compara con las tablas de direcciones MAC que se obtenían de los mismos switches. Ver Anexo 4.

La ubicación y direcciones MAC de las impresoras de red, de los servidores, de los routers y de otros equipos especiales, se obtuvo utilizando el *Sniffer* GFI LanGuard, que permite ingresar la dirección IP del host[2], y éste entrega el nombre del host, la dirección MAC, y otras informaciones como se ve en la Figura 1.13.

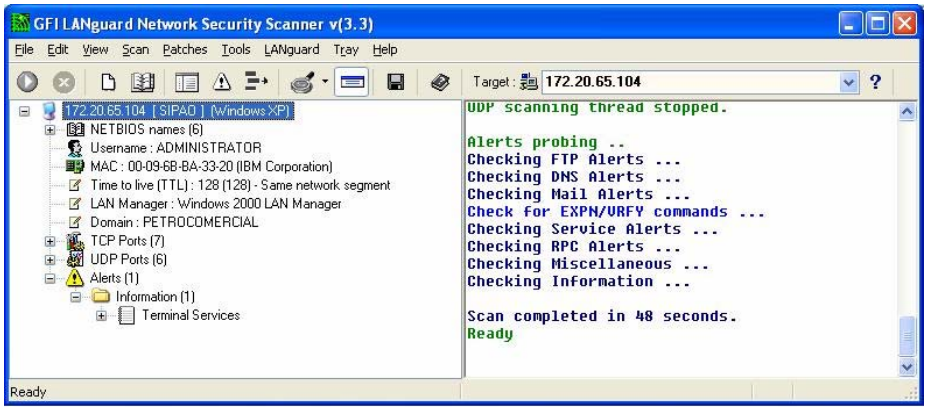


Figura 1.13 Sniffer GFI LanGuard

Pero si estos hosts se encontraban apagados no podían ser reconocidos, lo que llevo a utilizar otro *Sniffer* denominado BillSniff que monitoreaba toda la red un determinado tiempo, como se muestra en la Figura 1.14.

[2] Estación de trabajo, como por ejemplo una computadora

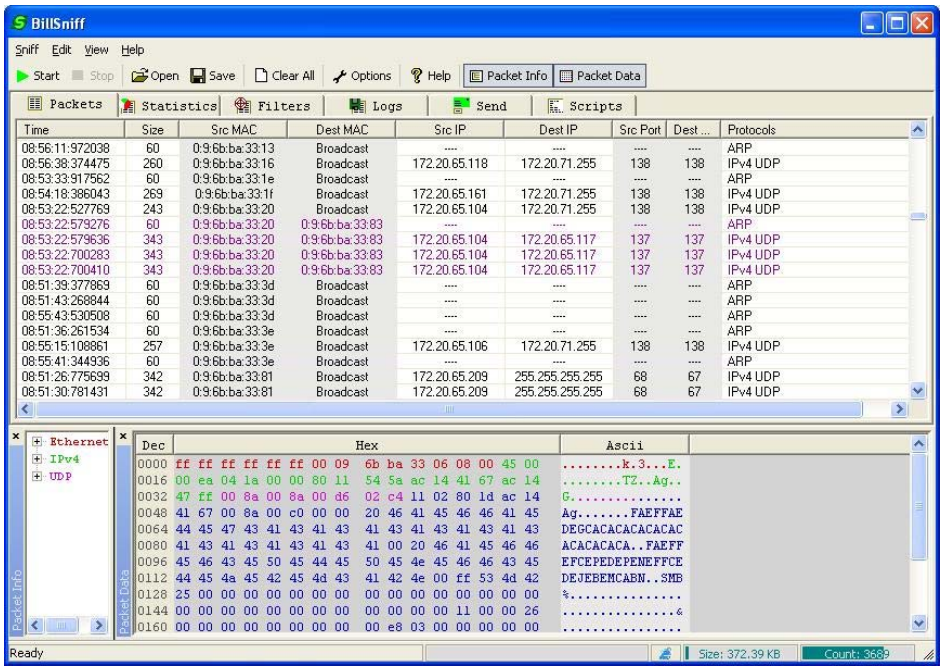


Figura 1.14 Sniffer BillSniff

Los equipos que lamentablemente no se encontraban conectados a un switch Cisco, se debía obtener la información en forma personal corroborando todo lo que se ha venido recopilando. Obteniendo así una base de datos sumamente completa que describe la ubicación dentro de los switches de todas las computadoras, teléfonos IP, equipos de red e impresoras, con sus respectivas direcciones MAC; así como también a que departamentos y a que personas pertenecen las PCs, teléfonos IP y otros equipos. Ver Anexo 3, Anexo 4 y Anexo 5.

El empeño que se ha puesto en levantar la información especialmente de la direcciones MAC de los host, es porque como luego veremos, estas bases de datos serán de mucha utilidad en el caso que se llegue a implementar VLANs dinámicas en base a direcciones MAC utilizando un Servidor de Políticas VLAN (VMPS). E incluso si se quiere dar seguridad a determinados puertos de los switches, restringiendo que computadoras (direcciones MAC) pueden o no conectarse a estos.

1.3.4 Rango de Direcciones IP de La Matriz

Ahora cabe hacer un pequeño análisis de cómo esta subneteada la red de Petrocomercial y que subred le corresponde a la Matriz, de acuerdo a su máscara.

Se utiliza la máscara y dirección de la interfaz local del router Vanguard 6455, nodo 220, que es el dispositivo que conecta a la red de la Matriz con el resto de la red de Petrocomercial. Realizamos una operación AND entre estas dos direcciones IP, para así obtener la dirección de subred que le corresponde a la Matriz.

172.20.0.0	dirección de red						
172.20.64.11/21	clase B	>>>>	10101100	.00010100	.01000000	.00001011	
255.255.248.0	máscara	>>>>	11111111	.11111111	.11111000	.00000000	and
172.20.64.0	dirección de sub-red	>>>>	10101100	.00010100	.01000000	.00000000	
			Sub-red			Host	

172.20.64.0	**Dirección de red**
172.20.64.1 – 172.20.71.254	**Rango de direcciones útiles (2046 hosts)**
172.20.71.255	**Dirección de broadcast**

En la Figura 1.15 se muestra el rango de direcciones que están siendo utilizadas y con que finalidad, dentro de la subred de la Matriz; con mayor detalle se puede ver en el Anexo 6, que indica que dirección IP esta utilizando cada equipo de red.

RANGO DE DIRECCIONES IP DE LA RED "LA MATRIZ"
(172.20.64.0/21)

172.20.64.0	**dirección de red**
172.20.64.1 … 172.20.64.19	**Comunicaciones (Routers, Firewall, RAS)**
172.20.64.20 … 172.20.64.29	**I-Series (AS/400's)**
172.20.64.30 … 172.20.64.49	**Direcciones para control del Firewall**
172.20.64.50 … 172.20.64.69	**Servidores**
172.20.64.70 172.20.64.99	**Impresoras de red**
…	
172.20.64.101 … 172.20.64.232	**Switches**
172.20.64.254	
172.20.64.255	
172.20.65.0	
172.20.65.1 .. 172.20.65.255	**DIRECCIONES UTILIZADAS POR EL DHCP PARA LA RED DE DATOS**
172.20.66.0 … 172.20.66.255	
172.20.67.0 … 172.20.67.255	
172.20.68.0 … 172.20.68.254	
172.20.68.255	
172.20.69.0	
172.20.69.1	**Dirección Estática (Central Telf. IP)**
…	
172.20.69.30 … 172.20.69.240	**Direcciones asignadas al DHCP de la Cental IP Mitel para los teléfonos IP**
172.20.69.241	
172.20.69.242	**Dirección estática del E2T (Central)**
… 172.20.69.255	
…	
172.20.71.0 …	
172.20.71.9	**Dirección Estática (Pcored6) - De baja**
…	
172.20.71.21	**Dirección Estática (Pcored1)**
… 172.20.71.254	
172.20.71.255	**dirección de broadcast**

Figura 1.15 Rango de Direcciones IP de la Red la Matriz

1.3.5 Nomenclatura de Dispositivos de Red

1.3.5.1 Nombre de los Switches

Tiene el siguiente formato **Pco_XYZ** donde:

Pco.- Es constante.

X.- Indica el edificio.

1.- Edificio El Rocio.

2.- Edificio Ex-Salesianos.

Y.- Indica el número de piso dentro del correspondiente edificio.

Z.- Indica el número de orden del switch. Si es ascendente comenzando desde 1 corresponde a la Serie Cisco Catalyst 3500 y 3550. Si es descendente comenzando desde 9 corresponde a la Serie Cisco Catalyst 2900.

En cuanto a las direcciones IP que en este momento están ocupadas por los switchs, se encuentran en la numeración: **172.20.64.N**, donde N corresponde al nombre XYZ del switch respectivo, por ejemplo Pco_153 tiene como dirección IP 172.20.64.153.

1.3.5.2 Etiquetado de los Switches

Todos los switches están etiquetados con el formato **SWXYZM** donde:

SW.- Es constante.

X.- Indica el edificio.

1.- Edificio El Rocio.

2.- Edificio Ex-Salesianos.

Y.- Indica el número de piso dentro del correspondiente edificio.

Z.- Indica el número de orden del switch. Si es ascendente comenzando desde 1 corresponde a la Serie Cisco Catalyst 3500 y 3550.Si es descendente comenzando desde 9 corresponde a la Serie Cisco Catalyst 2900.

M.- Corresponde a la marca del switch.

C.- Para el switch Cisco Catalyst

D.- Para el switch DLink.

I.- Para el switch IBM.

T.- Para el switch 3Com.

1.3.5.3 Nombre de los Servidores

Todos están nombrados por **PcoredS** donde S es el número del servidor.

1.3.6 Funcionamiento de la Telefonía en Petrocomercial

Es importante conocer cual es el funcionamiento de la telefonía, porque entre uno de los objetivos que se tiene planteado es el mejoramiento de la red de voz.

Las Centrales IP Mitel manejan extensiones analógicas por medio de Unidades de Servicio Analógico (ASUs), como es el caso de la central IP que se encuentra en la Matriz, que da servicio al edificio el Rocio y Ex-Salesianos, pero que también llega con este tipo de extensiones a otros terminales; por medio de tarjetas de voz para los usuarios distantes (FXS, *Foreign Exchange Station*) y tarjetas de voz cercanas a la central (FXO, *Foreign Exchange Office*), que poseen tanto los Multiplexores Bayly (ver Figura 1.16) como los routers Vanguard Motorota, aunque actualmente estos últimos no utilizan ambas tarjetas.

La forma de llegar a la mayoría de los terminales, es a través de líneas analógicas virtuales creadas dentro de la red WAN Frame Relay, siendo necesaria la configuración de una tabla de rutas de voz en cada uno de los routers Vanguard, y de la instalación de tarjetas FXS en los routers donde van a llegar cada una de las extensiones. Además estas líneas analógicas pueden ser troncales de cualquier Central IP, como es el caso de Beaterio (ver Figura 1.16)

De igual manera que con extensiones análogas, también se pueden llegar con extensiones IP de la Central Mitel de la Matriz a otros terminales, como: Beaterio (ver Figura 1.16), Santo Domingo, Osayacu y Oyambaro. Ver

Tabla 1.11

TELEFONOS IP REMOTOS DE LA CENTRAL MITEL - MATRIZ				
Extensión	**Lugar**	**Dirección MAC**	**Departamento**	**Unidad**
5106	Beaterio	08:00:0F:0E:74:88	Superint. Terminales	Superint. Terminales y Depósitos
5113	Beaterio	08:00:0F:0E:66:CC	Control de Calidad	Control de Calidad
5114	Beaterio	08:00:0F:0E:75:FC	Inspecciión técnica	Inspección Técnica
5121	Beaterio	08:00:0F:0E:75:FB	Telecomunicaciones	Sistemas y Telecomunicaciones
5236	Sto. Domingo	08:00:0F:0E:64:E2	Jefatura de Operaciones	Superint. Polid. Esm-Sto.Dom.-Quito-Mac.
5237	Sto. Domingo	08:00:0F:0E:99:8C	Jef. Mtto. De Línea	Superint. Polid. Esm-Sto.Dom.-Quito-Mac.
5444	Osayacu	08:00:0F:0E:73:A8	Superintendencia	Superint. Poliducto Shushu.-Quito
5472	Oyambaro	08:00:0F:0E:72:A5	Secretaría	Superint. Terminales y Depósitos

Tabla 1.11 Teléfonos IP Remotos de la Central Mitel - Matriz

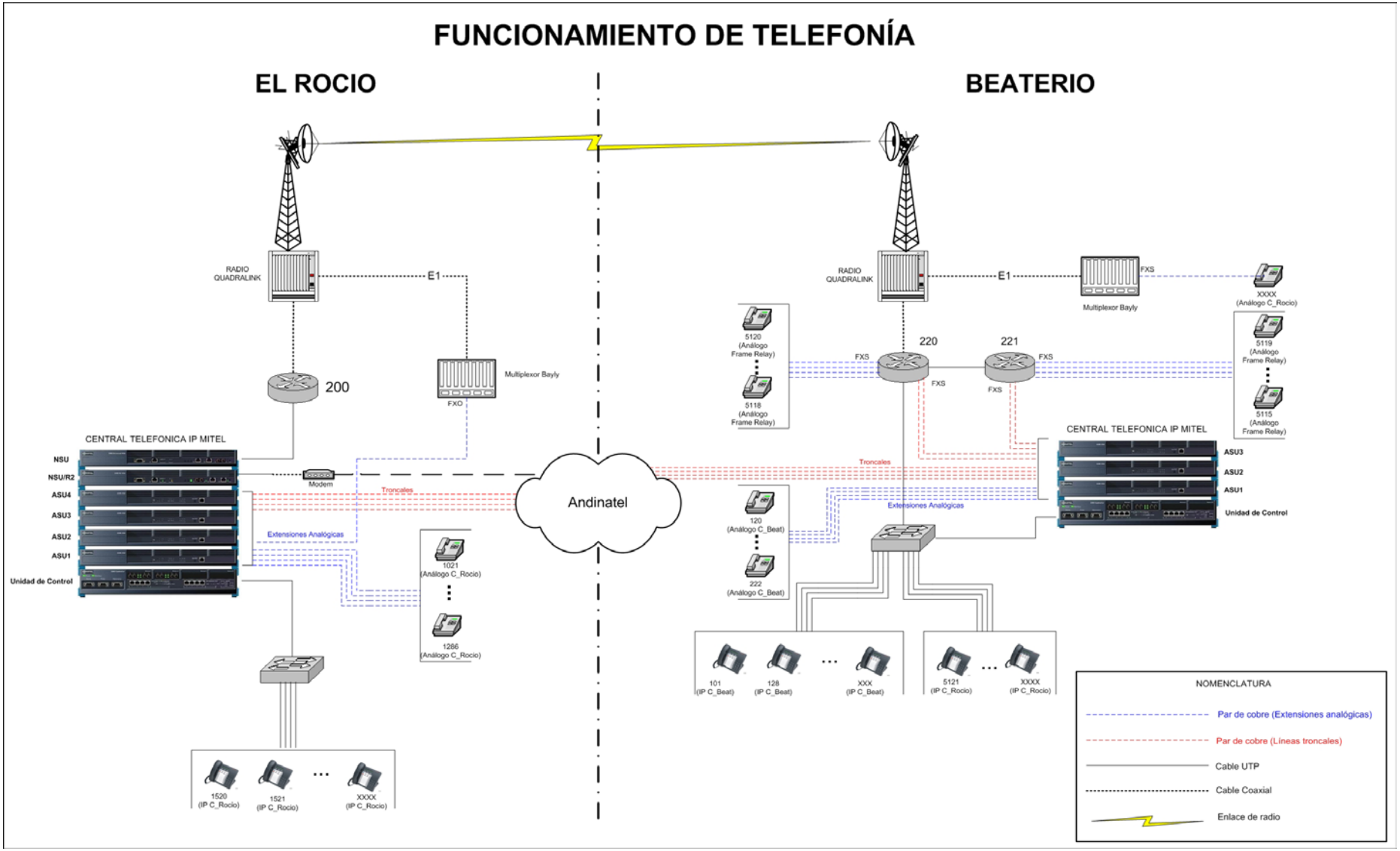


Figura 1.16 Funcionamiento de la Telefonía en Petrocomercial

1.4 RED DE BEATERIO

Esta red local es la segunda más grande e importante de la Regional Norte después de la red de la Matriz, por ser uno de los terminales más grande a nivel operativo. La función principal de esta terminal es el almacenamiento y despacho de combustible.

1.4.1 Interconexión de los Elementos Activos de Red de Beaterio

La red de Beaterio tiene un backbone físico formado por fibra óptica, lo cual es beneficioso, pero lastimosamente utiliza convertidores de fibra a UTP, que reducen las ventajas que nos ofrece este medio, y todo esto es debido a que la mayoría de los equipos son switches sin puertos para fibra y sin inteligencia. Ver Figura 1.17

En resumen los switches que se utilizan en Beaterio son:

SWITCHES DE BEATERIO					
Nombre	**Dirección IP**	**Switch**	**Modelo**	**Version IOS**	**Ubicación**
Pco_131	172.20.129.131	Cisco Catalyst 3550 Series	WS-3550-24-PWR-SMI	12.1 (13) EA1a	Telecomunicaciones
Pco_191	172.20.129.191	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	12.0 (5) WC3b	Jef. Terminal
Pco_134	172.20.129.134	Cisco Catalyst 2900 XL Series	WS-C2912-XL	12.0 (5.2) XU	Comercializadora
		DLINK 10/100	(8 puertos)		Comercializadora
		DLINK 10/100	(8 puertos)		Polid. Q.A.R.
		DLINK 10/100	(8 puertos)		Seguridad Industrial
		DLINK 10/100	(5 puertos)		Mtto. Eléctrico
		3COM 10/100	(8 puertos)		Bodega
		CNET	(8 puertos)		Reductora
		CNET	(8 puertos)		Control de Calidad

Tabla 1.12 Switches de Beaterio

Además se utiliza el Router Vanguard 6455 (nodo 220), para comunicarse con la red WAN de Petrocomercial, y 2 *Wireless Bridge*[3] 3COM (*Spread Spectrum*[4]) para llegar a Jet-Fuel desde Telecomunicaciones. Ver Figura 1.17

[3] Puente Inalámbrico
[4] Espectro ensanchado

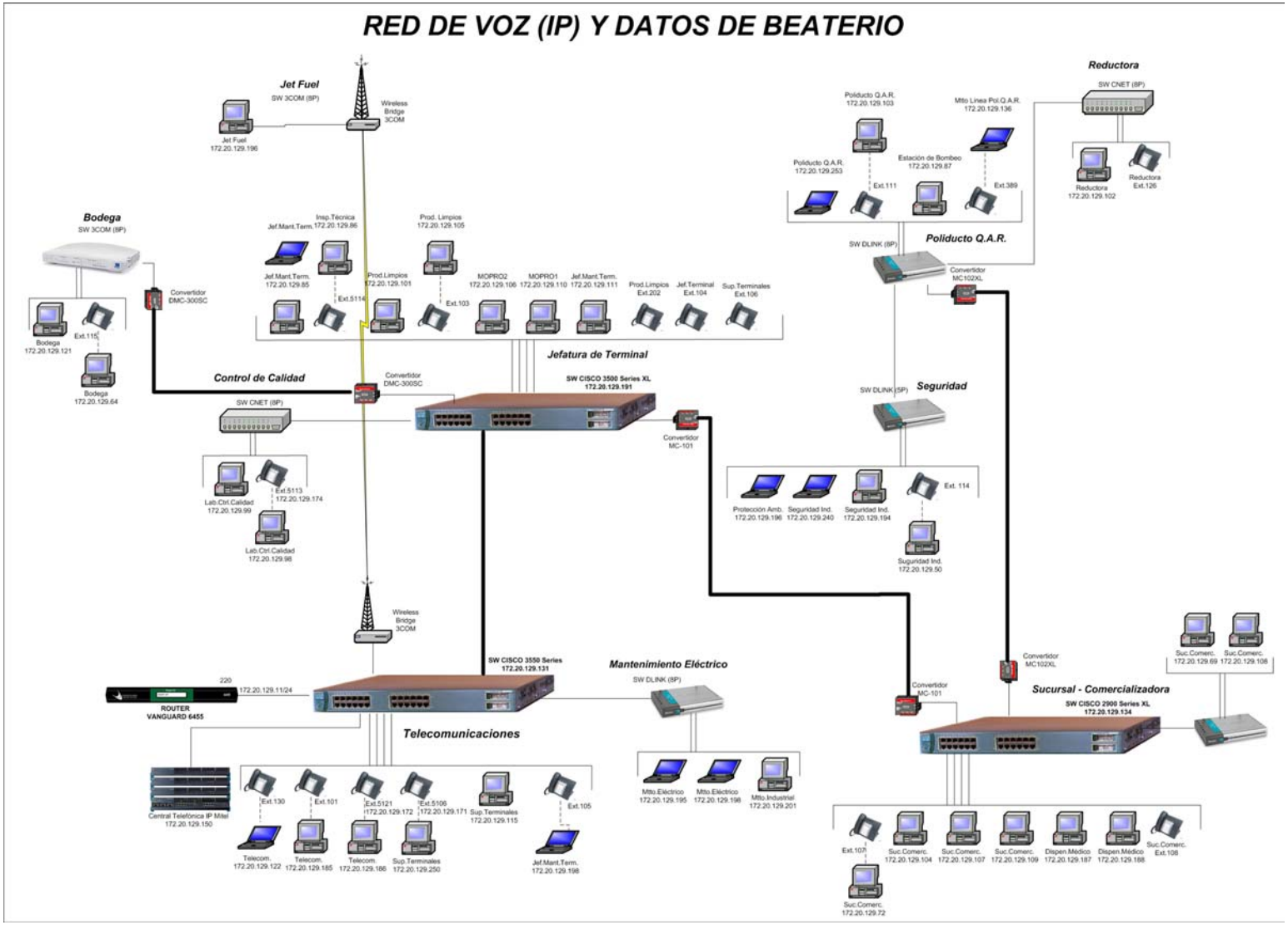


Figura 1.17 Red de Voz y Datos de Beaterio

1.4.2 Equipos de la Red de Beaterio

En la Tabla 1.13 se detalla la cantidad de computadoras (PCs) y teléfonos IP por cada departamento, además de contabilizar el número de teléfonos IP independientes, (es decir que no están conectados a una computadora), para determinar el número total de puntos de red necesarios.

Cantidad de estaciones de trabajo en Beaterio					
Switch:	**Departamento:**	**PC's**	**Telf. IP**	**Telf IP ind**	**Ptos red**
Cisco Catalyst 3550 Series	Telecomunicaciones	3	3		3
	Superintencia de Terminales	2	2	1	3
Cisco Catalyst 3500 XL Series	Jefatura de Terminal		1	1	1
	Jefatura de Mantenimiento de Terminal	4	2	1	5
	Productos Limpios	2	2	1	3
	MOPRO	2			2
	Inspección Técnica	1	1		1
Cisco Catalyst 2900 XL Series	Sucursal - Comercializadora	4	2	1	5
	Dispensario Médico	2			2
DLINK 10/100	Comercializadora	2			2
DLINK 10/100	Mantenimiento Eléctrico	2			2
	Mantenimiento Industrial	1			1
DLINK 10/100	Superint. Poliducto Q.A.R.	2	1		2
	Mtto. De Línea de P.Q.A.R.	1	1	1	2
	Operaciones (Estación de Bombeo)	1			1
DLINK 10/100	Protección Ambiental	1			1
	Seguridad Industrial	3	1	1	4
CNET	Reductora	1	1	1	2
3COM 10/100	Bodega	2	1		2
CNET	Control de Calidad	2	1		2
Wireless Bridge 3COM	Jet Fuel	1			1
TOTAL:		**39**	**19**	**8**	**47**

Tabla 1.13 Cantidad de Estaciones de Trabajo en Beaterio

De estos 19 teléfonos IP, cuatro de ellos vienen de la Central IP de la Matriz, estos teléfonos son:

Telefonos IP que llegan desde La Matriz a Beaterio			
Extensión	**Dirección MAC**	**Departamento**	**Dirección IP**
5106	08:00:0F:0E:74:88	Superint. Terminales	172.20.129.171
5113	08:00:0F:0E:66:CC	Control de Calidad	172.20.129.174
5114	08:00:0F:0E:75:FC	Inspecciión técnica	172.20.129.175
5121	08:00:0F:0E:75:FB	Telecomunicaciones	172.20.129.172

Tabla 1.14 Teléfonos IP que llegan desde la Matriz a Beaterio

Estas extensiones tienen direcciones IP estáticas, para ser controladas por la Central de la Matriz, y coinciden dentro del rango de direcciones IP del DHCP de la Central de Beaterio.

1.4.3 Rango de Direcciones IP de Beaterio

La asignación de direcciones IP de las computadoras de Beaterio actualmente es en forma estática, y obviamente para los switches, el router, y el controlador de la Central IP.

Direcciones IP de Beaterio - Quito Red: 172.20.129.0/24	
Detalle	**Descripción**
…	
172.20.129.11	Router Motorola Vanguard 6455 (220)
…	
172.20.129.131	Switch Cisco Catalyst 3550 Series
…	
172.20.129.134	Switch Cisco Catalyst 2900 XL Series
…	
172.20.129.150	Central Telefónica MITEL
172.20.129.151 … 172.20.129.180	RANGO DEL DHCP DE LA CENTRAL IP DE BEATERIO
…	
	E2T de la Central Telefónica Mitel
…	
172.20.129.191	Switch Cisco Catalyst 3500 XL Series
…	
172.20.129.254	Router Motorola Vanguard 6455 (221)

Nota:	El resto de direcciones es para asignar direcciones estáticas a las computadoras

Tabla 1.15 Rango de Direcciones de Beaterio

Si se desea el detalle de las direcciones IP de las computadoras y su ubicación, recurrir al Anexo 7, y para información acerca de la ubicación de todos los teléfonos IP de Beaterio recurrir al Anexo 8.

1.5 RED DE SANTO DOMINGO

1.5.1 Interconexión de los Elementos Activos de Red de Santo Domingo

Para dar servicio a Sucursal, se lo realiza desde el cuarto de comunicaciones por medio de modems denominados "*Black Box*", que utilizan 4 hilos de cobre para comunicarse entre ellos. Para llegar a Jefatura de Mantenimiento de Línea y al Supervisor de Operaciones se utilizan enlaces S*pread Spectrum* desde el cuarto de comunicaciones, y desde este mismo punto se llega a Superintendencia de Terminal usando cable UTP; y solamente a Jefatura de Terminal se llega a través de fibra óptica desde Sucursal. Ver Figura 1.18.

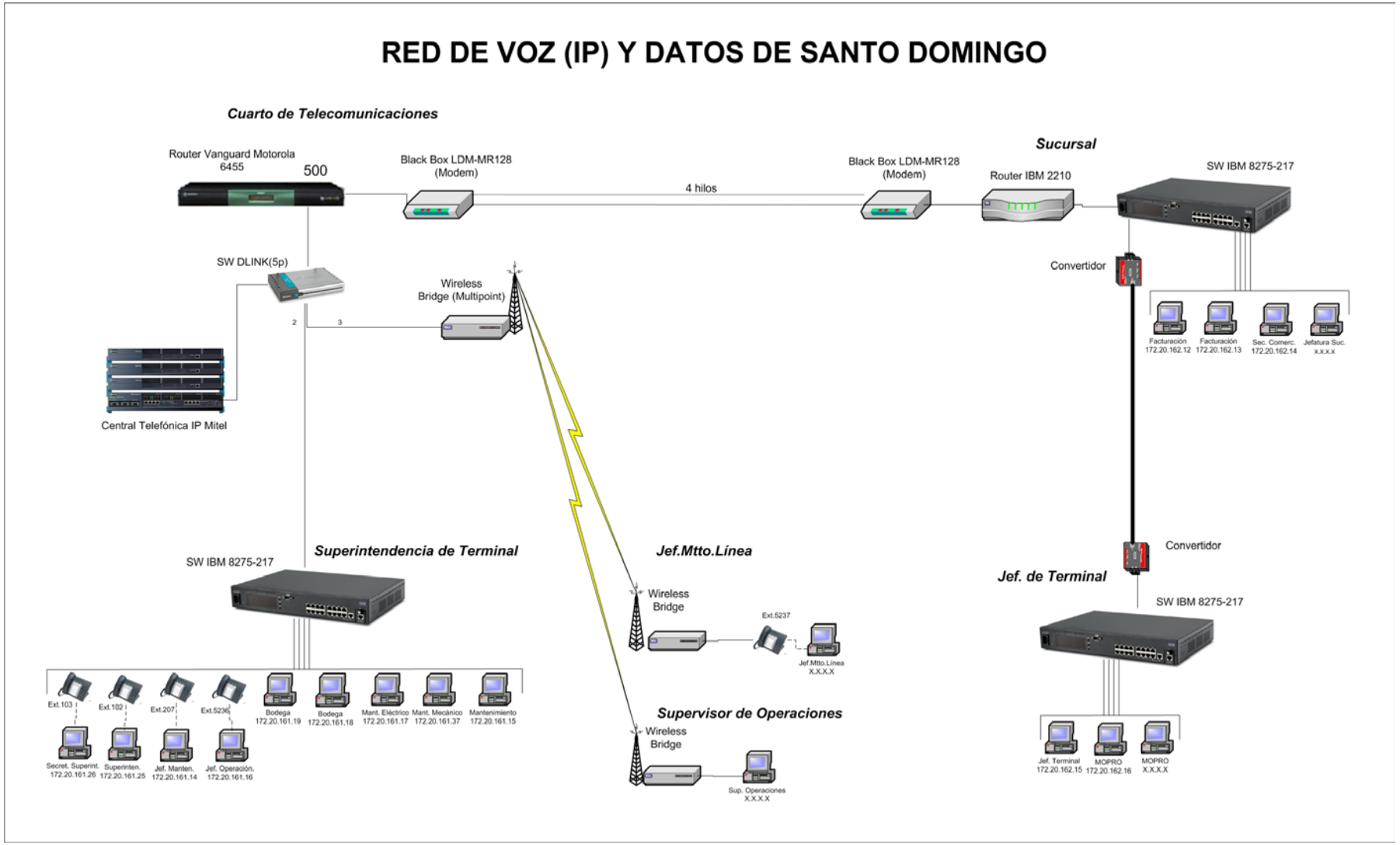


Figura 1.18 Red de Voz y Datos de Santo Domingo

La red de Santo Domingo consta de los siguientes equipos:

Equipos de Santo Domingo		
Cantidad	**Equipos**	**Modelo**
3	Switch IBM 10/100	8275-217
1	Switch DLINK	5 puertos
1	Router Motorola Vanguard	6455
1	Router IBM	2210
1	Wireless Bridge 3COM	Multipoint
2	Wireless Bridge 3COM	Singlepoint
2	Modem Black Box	LDM-MR128

Tabla 1.16 Equipos de Santo Domingo

Se utiliza el Router Vanguard 6455 (nodo 500), para comunicarse con la red WAN de Petrocomercial.

1.5.2 Equipos de la red de Santo Domingo

En la siguiente tabla se detalla la cantidad de computadoras, teléfonos IP por cada departamento y el número total de puntos de red.

Cantidad de estaciones de trabajo en Santo Domingo				
Equipos	**Departamento**	**PC's**	**Telf IP**	**Ptos red**
Switch IBM 8275-217 (1)	Jef. de Mantenimiento	1	1	2
	Jef. de Operación	1	1	2
	Superintendencia	2	2	4
	Mtto. Mecánico	1		1
	Mtto. Eléctrico	1		1
	Bodega	2		2
	Mantenimiento			
Switch IBM 8275-217 (2)	Facturación	2		2
	Comercialización			
	Jefatura Sucursal			
	Jefatura de Terminal			
	MOPRO			
	MOPRO			
Wireless Bridge (1)	Jef. Mtto. de Línea		1	1
Wireless Bridge (2)	Superint. Operaciones			
TOTAL:		**10**	**5**	**15**

Tabla 1.17 Cantidad de Estaciones de Trabajo en Santo Domingo

De los cinco teléfonos IP, dos de ellos vienen de la Central IP de la Matriz.

1.5.3 Rango de Direcciones IP de Santo Domingo

La asignación de direcciones IP para las computadoras de Santo Domingo es en forma estática, así como para los routers, y el controlador de la Central IP.

Direcciones IP de Santo Domingo Red: 172.20.161.0/24 y 172.20.162.0/24	
Detalle	**Descripción**
172.20.161.11	Router Motorola Vanguard 6455 (220)
172.20.161.14	PC de Jef. de Mantenimiento
172.20.161.15	PC de Mantenimiento
172.20.161.16	PC de Jef. de Operación
172.20.161.17	PC de Mtto. Eléctrico
172.20.161.18	PC de Bodega
172.20.161.19	PC de Bodega
172.20.161.25	PC de Secret. Superintendencia
172.20.161.26	PC de Superintendencia
172.20.161.37	PC de Mtto. Mecánico
172.20.161.XX	PC de Jef. Mtto. de Línea
172.20.161.XX	PC de Superint. Operaciones
172.20.161.20	Central Telefónica MITEL
172.20.161.21 ... 172.20.161.40	RANGO DEL DHCP DE LA CENTRAL IP DE SANTO DOMINGO para los telefonos IP
172.20.162.11	Router Motorola Vanguard 6455 (220)
172.20.162.12	PC de Facturación
172.20.162.13	PC de Facturación
172.20.162.14	PC de Comercialización
172.20.162.15	PC de Jefatura de Terminal
172.20.162.16	PC de MOPRO
172.20.162.XX	PC de MOPRO
172.20.162.XX	PC de Jefatura Sucursal

Tabla 1.18 Direcciones IP de Santo Domingo

1.6 RED DE ESMERALDAS

1.6.1 Interconexión de los Elementos Activos de Red de Esmeraldas

Para llegar a Sucursal y a Cabecera se utilizan radio enlaces desde Balao PCO, mientras que para llegar a Petroindustrial se utiliza un enlace *Spread Spectrum* desde Sucursal. Además vale recalcar que la red que existe en Petroindustrial no es preocupación de Petrocomercial, simplemente se les provee de los medios de comunicación. Ver Figura 1.19. Los equipos que se utilizan en Esmeraldas son:

Equipos de Esmeraldas		
Cantidad	**Equipos**	**Modelo**
2	Router Motorola Vanguard	6455
1	Router Motorola Vanguard	6435
1	Switch IBM	8275-217
1	Switch 3COM	8 puertos

Tabla 1.19 Equipos de Esmeraldas

Se utiliza el Router Vanguard 6455 (nodo 600), de Balao PCO, para comunicarse con la red WAN de Petrocomercial.

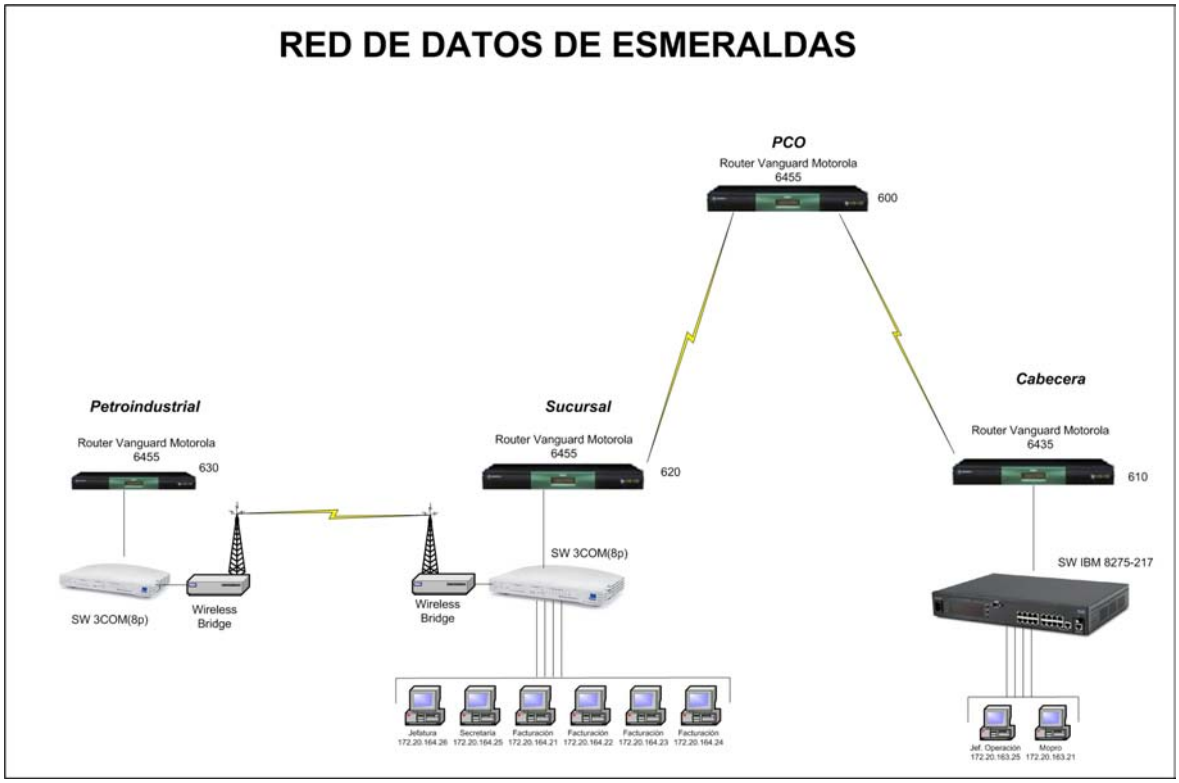


Figura 1.19 Red de Datos de Esmeraldas

1.6.2 Equipos de la Red de Esmeraldas

A continuación se detalla la cantidad de computadoras por cada departamento.

Cantidad de estaciones de trabajo en Esmeraldas		
Equipos	**Departamento**	**PC's**
Switch IBM 8275-217	Jef. de Operación	1
	MOPRO	1
Switch IBM 8275-217 (2)	Jefatura	1
	Secretaría	1
	Facturación	4
TOTAL:		**8**

Tabla 1.20 Cantidad de Estaciones de Trabajo en Esmeraldas

1.6.3 Rango de Direcciones IP de Esmeraldas

La asignación de direcciones IP de las computadoras de Esmeraldas es en forma estática. Ver Tabla 1.21.

Direcciones IP de Esmeraldas Red: 172.20.163.0/24 y 172.20.164.0/24	
Detalle	**Descripción**
172.20.163.11	Router Motorola Vanguard 6455 (610)
172.20.163.21	PC de MOPRO
172.20.163.25	PC de Jefatura de Operaciones
172.20.164.11	Router Motorola Vanguard 6455 (620)
172.20.164.21	PC de Facturación
172.20.164.22	PC de Facturación
172.20.164.23	PC de Facturación
172.20.164.24	PC de Facturación
172.20.164.25	PC de Secretaría
172.20.164.26	PC de Jefatura

Tabla 1.21 Direcciones IP de Esmeraldas

1.7 RED DE AMBATO

1.7.1 Interconexión de los Elementos Activos de Red de Ambato

El backbone de la red de Ambato utiliza cable UTP, para llegar a la Jefatura de Terminal, a Sucursal y a Reductora.

Se utiliza el Router Vanguard 6455 (nodo 300), para comunicarse con la red WAN de Petrocomercial, ver Figura 1.20. Los equipos que se utilizan en Ambato son:

Equipos de Ambato		
Cantidad	**Equipos**	**Modelo**
1	Router Motorola Vanguard	6455
2	Switch IBM	8237
1	Switch 3COM	8 puertos

Tabla 1.22 Equipos de Ambato

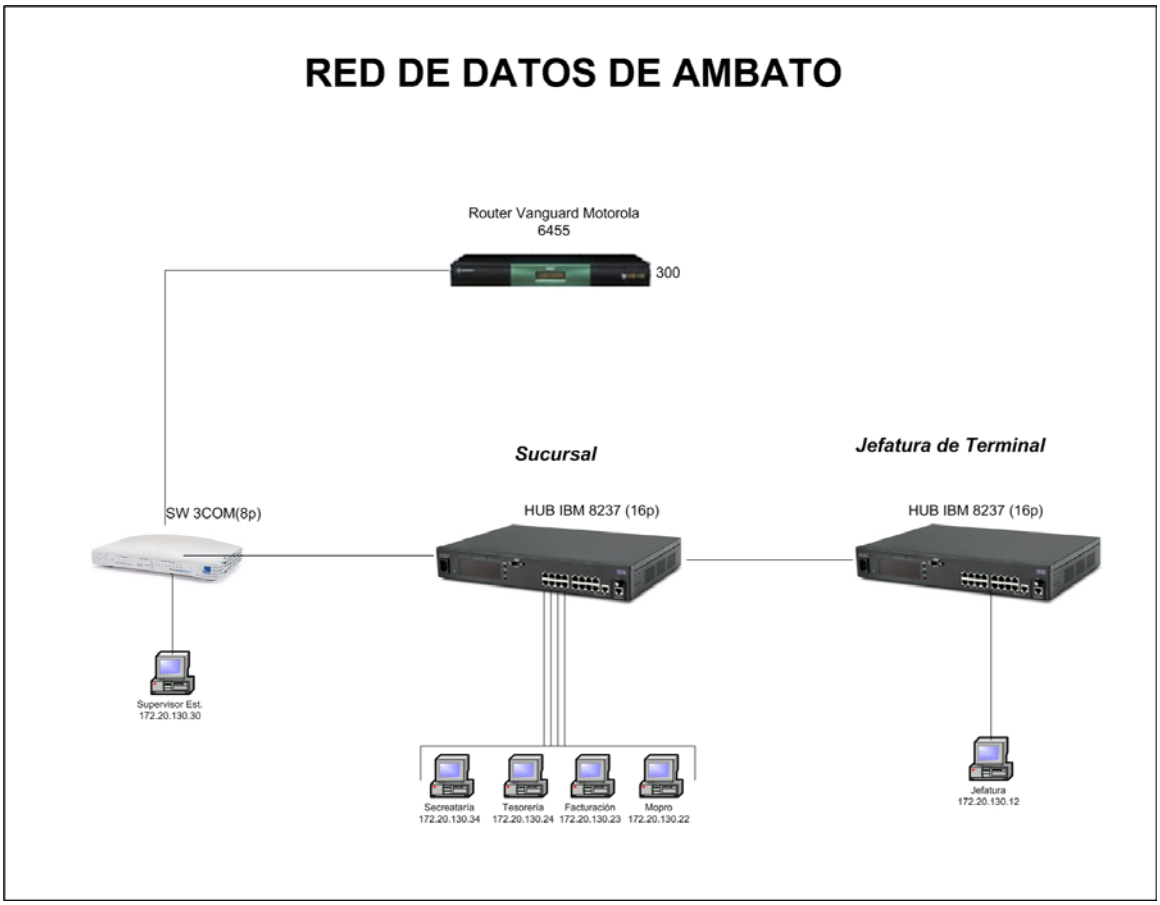


Figura 1.20 Red de Datos de Ambato

1.7.2 Equipos de la Red de Ambato

A continuación se detalla la cantidad de computadoras por cada departamento.

Cantidad de estaciones de trabajo en Ambato		
Equipos	**Departamento**	**PC's**
Switch IBM 8237 (1)	Secretaría	1
	Tesorería	1
	Facturación	1
	MOPRO	1
Switch IBM 8237 (2)	Jefatura	1
Switch 3COM	Supervisor de estación	1
TOTAL:		**6**

Tabla 1.23 Cantidad de Estaciones de Trabajo en Ambato

1.7.3 Rango de Direcciones IP de Ambato

La asignación de direcciones IP de las computadoras de Ambato es en forma estática. Ver Tabla 1.24.

Direcciones IP de Ambato Red: 172.20.130.0/24	
Detalle	**Descripción**
172.20.130.11	Router Motorola Vanguard 6455 (300)
172.20.130.12	PC de Jefatura
172.20.130.22	PC de MOPRO
172.20.130.23	PC de Facturación
172.20.130.24	PC de Tesorería
172.20.130.30	PC de Supervisor de estación
172.20.164.34	PC de Secretaría

Tabla 1.24 Direcciones IP de Ambato

1.8 RED DE SHUSHUFINDI

1.8.1 Interconexión de los Elementos Activos de Red de Shushufindi

Para llegar tanto al Poliducto Cabecera como a la Sucursal de Comercialización se utilizan radio enlaces desde Shushufindi Petroindustrial.

Se utiliza el Router Vanguard 6455 (nodo 820), para comunicarse con la red WAN de Petrocomercial, ver Figura 1.21. Los equipos que se utilizan en Shushufindi son:

Equipos de Shushufindi		
Cantidad	**Equipos**	**Modelo**
1	Router Motorola Vanguard	6455
2	Router Motorola Vanguard	6435
2	Switch 3COM	8 puertos

Tabla 1.25 Equipos de Shushufindi

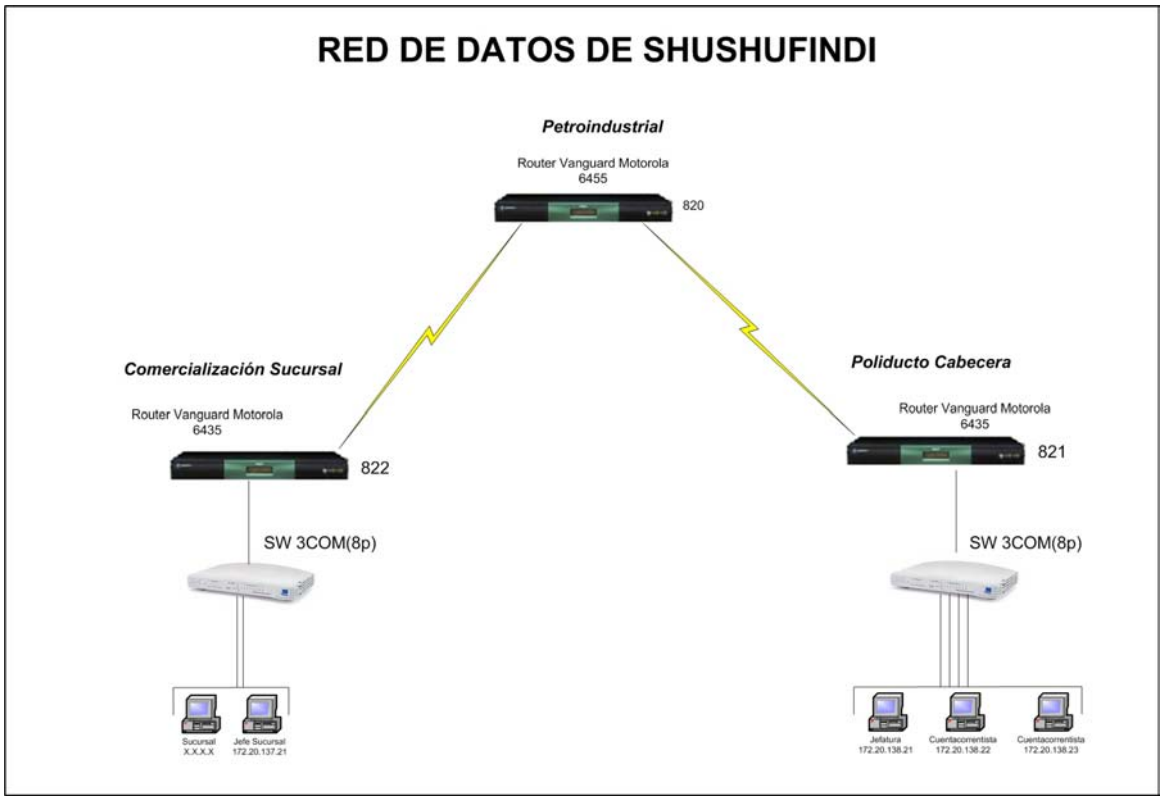


Figura 1.21 Red de Datos de Shushufindi

1.8.2 Equipos de la Red de Shushufindi

A continuación se detalla la cantidad de computadoras por cada departamento.

Cantidad de estaciones de trabajo en Shushufindi		
Equipos	**Departamento**	**PC's**
Switch 3COM (1)	Jefatura	1
	Cuentacorrentista	1
	Cuentacorrentista	1
Switch 3COM (2)	Sucursal	1
	Jefatura de Sucursal	1
TOTAL:		**5**

Tabla 1.26 Cantidad de Estaciones de Trabajo en Shushufindi

1.8.3 Rango de Direcciones IP de Shushufindi

La asignación de direcciones IP de las computadoras de Shushufindi es en forma estática. Ver Tabla 1.27

Direcciones IP de Shusufindi Red: 172.20.137.0/24 y 172.20.138.0/24	
Detalle	**Descripción**
172.20.137.11	Router Motorola Vanguard 6435 (822)
172.20.137.21	PC de Jefatura de Sucursal
172.20.137.xx	PC de Sucursal
172.20.138.11	Router Motorola Vanguard 6435 (821)
172.20.138.21	PC de Jefatura
172.20.138.22	PC de Cuentacorrentista
172.20.138.23	PC de Cuentacorrentista

Tabla 1.27 Direcciones IP de Shushufindi

1.9 RESUMEN DE LA CANTIDAD DE HOSTS DE LAS REDES LOCALES

El resumen de la cantidad de hosts en cada una de las redes locales de la Regional – Norte de Petrocomercial se muestra en la Tabla 1.28.

Cantidad de Hosts de la Regional Norte				
	# PC's	# Tel IP	# Impr	# Total Hosts
Matriz	275	138	15	428
Beaterio	39	19		58
Santo Domingo	10	5		15
Esmeraldas	8			8
Ambato	6			6
Shushufindi	5			5
Aeropuerto	2			2
Gasolinera	8			8
Oyambaro	5			5
Osayacu	5			5
Riobamba	3			3
Corazón	1			1
Chalpi	1			1
Total:				**545**

Tabla 1.28 Resumen de la cantidad de hosts de las redes locales

De acuerdo al presente resumen, el 90% de hosts en la Regional Norte se concentra en las redes locales de la Matriz y Beaterio. Por lo tanto este proyecto enfocará sus objetivos planteados en estas dos redes locales. La cantidad de hosts es tan reducida en las otras redes, que no tiene sentido implementar VLANs en ellas, y además la mayor parte de los equipos (switches) en estas redes no soportan la configuración de VLANs.

CAPITULO II

FUNDAMENTOS TEÓRICOS

2.1 CONCEPTOS GENERALES

2.1.1 Modelo OSI[1]

Es un modelo de red descriptivo de siete capas definido por la ISO[2], que asegura compatibilidad e interoperatibilidad entre varias tecnologías de red producidas por diferentes compañías. Lo que permite trabajar de manera independiente sobre funciones de red separadas y por ende disminuir su complejidad y acelerar su evolución.

Este modelo esta formado por siete capas, cada una de las cuales realiza funciones diferentes, que son:

1) **Capa Física:** Especifica voltajes, conectores, tazas de transmisión, medios de transmisión, etc.
2) **Capa de Enlace de Datos:** Utiliza las direcciones MAC para acceder a las estaciones finales, notifica errores pero no los corrige, etc.
3) **Capa de Red:** Determina el mejor camino, utilizando direccionamiento lógico (IP).
4) **Capa de Transporte:** Provee una confiable o no confiable entrega de datos, reensambla los segmentos que llegan en desorden, etc.
5) **Capa de Sesión:** Establece, maneja y termina sesiones entre aplicaciones, asigna puertos lógicos, etc.

[1] Open System Interconnection
[2] International Organization for Standarization

6) **Capa de Presentación:** Traduce entre varios formatos de datos, encriptamiento, compresión, etc.
7) **Capa de Aplicación:** Provee protocolos y software al servicio del usuario (Navegadores WEB, correo electrónico, etc.).

Para que los datos viajen desde un origen a su destino, cada capa del modelo OSI en el origen debe comunicarse con su respectiva capa en el destino. Esta comunicación es conocida como *peer-to-peer*. Durante este proceso, los protocolos de cada capa intercambian información denominada *Protocol Data Units (PDUs)*. Ver Figura 2.1

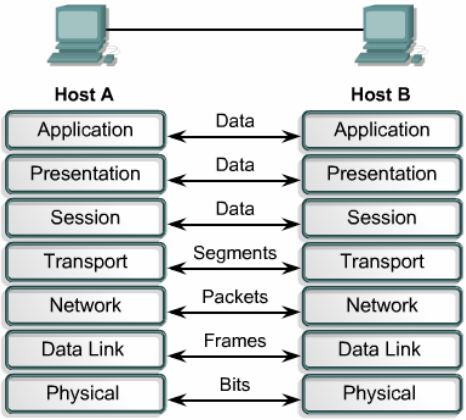


Figura 2.1 Comunicación Peer-to-Peer[3]

Encapsulación, es el método que añade cabeceras y *trailers*[4] a los datos que se mueven hacia abajo de la pila de capas del modelo OSI. El dispositivo receptor desnuda la cabecera, que contiene direcciones para esa capa (des-encapsulación).

2.1.2 Dispositivos de Red

Existen dos clasificaciones, la primera clasificación son los **dispositivos de usuario final,** como por ejemplo computadoras, impresoras, scanners y otros dispositivos que provean servicios directamente al usuario. Estos dispositivos son conectados físicamente a la red usando una *Network Interface Card* [5](NIC) que tiene su propio código o dirección MAC. La segunda clasificación son los dispositivos de red.

[3] Figura editada de Cisco CCNA1, Peer-to-peer communications
[4] Campo añadido al final del paquete de datos
[5] Tarjeta de Interface de Red

Los **dispositivos de red** proveen la comunicación entre dispositivos de usuario final. Como por ejemplo:

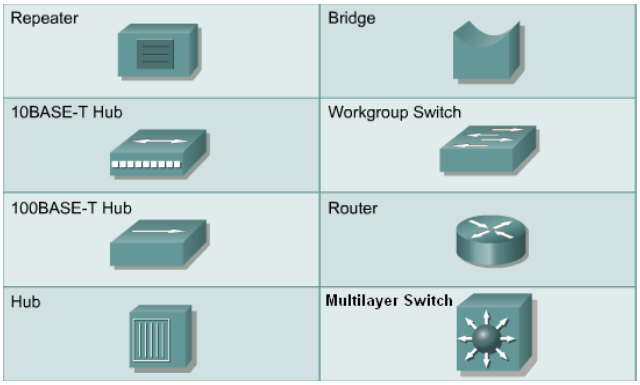


Figura 2.2 Iconos de los Dispositivos de Red[6]

2.1.2.1 Repetidor

Es un dispositivo de red usado para regenerar una señal. Regeneran señales analógicas o digitales distorsionadas por la pérdida de transmisión debido a la atenuación. Es un dispositivo de capa 1.

2.1.2.2 Hub

Dispositivo de capa 1, que permite la concentración de varios dispositivos dentro de un solo dominio de colisión o segmento. Regenera y amplifica las señales de datos para todos los dispositivos conectados, excepto para el dispositivo que originalmente envió la señal. También es conocido como un repetidor multipuerto, que extiende los dominios de colisión.

2.1.2.3 Bridge

Es un dispositivo de capa 2 que separa dominios de colisión, porque analiza las direcciones MAC para determinar si las tramas de datos pueden o no cruzar entre dos segmentos de red. Para lograr esto el bridge aprende las direcciones MAC de los dispositivos en cada segmento conectado. Además este dispositivo puede convertir formatos de transmisión de datos, lo cual no puede realizar un switch de capa 2.

[6] Figura editada de Cisco CCNA1, Networking Devices

2.1.2.4 Switch

También es un dispositivo de capa 2 y puede ser referido como un bridge multipuerto. Los switches toman las decisiones de envío basadas en las direcciones MAC contenidas dentro de las trama de datos transmitidas. Los switches aprenden las direcciones MAC de los dispositivos conectados a cada puerto, a través de la lectura de las direcciones MAC origen que se encuentran en las tramas que ingresan al switch, luego esta información es ingresada dentro de la tabla de conmutación que es almacenada en la CAM[7].

El switch se fija en la dirección MAC de destino contenida en la cabecera de la trama, para enviar la trama a la apropiada interfaz o puerto, basado en las direcciones MAC de la tabla de conmutación. Cuando el destino de la trama (dirección MAC de destino de la trama) es desconocido para el switch, éste inunda con la trama a todos los puertos excepto el puerto que lo recibió. Esto se conoce como **proceso *"FLODDING"* de un switch**. Y una vez que se recibe una respuesta, el switch almacena la nueva dirección en la CAM.

Los switches crean un circuito virtual entre dos dispositivos conectados que quieren comunicarse. Cuando este circuito virtual ha sido creado, un camino de comunicación dedicado es establecido entre los dos dispositivos. Esto crea un ambiente libre de colisiones entre el origen y el destino lo cual implica la máxima utilización del ancho de banda disponible. Los switches son capaces de manejar múltiples conexiones de circuitos virtuales en forma simultánea. Ver Figura 2.3

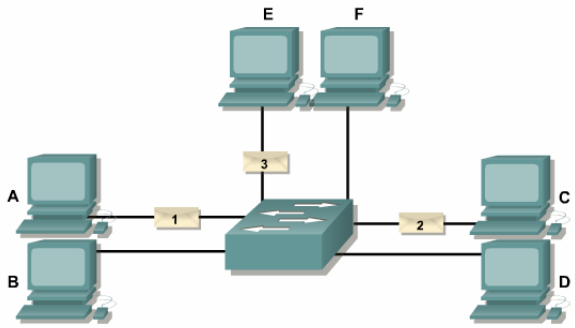


Figura 2.3 Transmisiones Simultáneas en un Switch[8]

[7] Content Addressable Memory
[8] Figura de Cisco CCNA3, VLAN basics

Cada puerto del switch representa un solo dominio de colisión, lo cual se conoce como microsegmentación. La desventaja de todos los dispositivos de capa 2, es que ellos envían tramas broadcast a todos los dispositivos conectados a sus puertos.

2.1.2.5 Router

Es un dispositivo de capa 3 que toma decisiones basadas en direcciones de red. Estos utilizan tablas de enrutamiento para almacenar estas direcciones de capa 3. Los routers se encargan de elegir el mejor camino para enviar los datos a su destino y conmutar o enrutar los paquetes al puerto de salida adecuado.

Los routers dividen tanto dominios de broadcast como dominios de colisión. Además, son los dispositivos de mayor importancia para regular el tráfico, porque proveen políticas adicionales para la administración de la red con filtrado de paquetes para la seguridad. También dan acceso a redes de área amplia (WAN), las cuales están destinadas a comunicar o enlazar redes de área local (LANs) que se encuentran separadas por grandes distancias.

El router también tiene la capacidad de convertir formatos de transmisión de datos, lo que quiere decir que puede conectar diferentes tipos de redes, como por ejemplo FDDI[9], Ethernet, Token Ring, etc.

Algunas ventajas de los switch de capa 2 frente a los routers han determinado la idea de difundir el switch y usar el router solo una vez ("un switch cuando se puede, un router cuando se debe"). El switch tiene menor latencia, mayor capacidad de tráfico (*Throughput*), fácil administración (concepto de gestión "*plug and play*") y menor costo por puerta.

[9] Fiber Distributed Data Interface

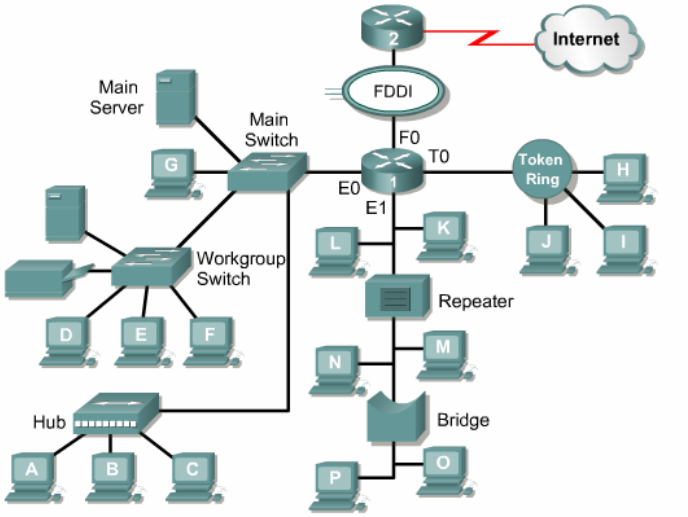


Figura 2.4 Ejemplo de la Interconexión de Dispositivos de Red[10]

2.1.2.6 Switch multilayer

Un switch multilayer es la combinación de la conmutación tradicional de capa 2 con la operación de enrutamiento de capa 3 en un solo dispositivo, mediante acciones de hardware de alta velocidad. En tanto que en un router el enrutamiento se lo realiza mediante técnicas de software lentas. Este switch se fundamenta en circuitos del tipo **ASIC**[11].

Los switches multilayer son más rápidos y baratos que los routers. Aunque algunos switches multilayer carecen de modularidad y flexibilidad que usualmente tienen asociados los routers.

Un switch de capa 4 realiza funciones de conmutación de paquetes tomando en cuenta el *socket* (dirección IP y puerto TCP/UDP). De esta forma se puede tener acceso al tipo de servicio (capa de aplicación) transportado y realizar operaciones de prioridad del tráfico con mayor precisión (política de calidad de servicio).

En la actualidad existen switches que pueden manejar información relacionada desde la capa 2 (enlace de datos) hasta la capa 7 (aplicación) del modelo OSI.

[10] Figura de Cisco CCNA1, Network Topology
[11] Application-Specific Integrated Circuit

2.1.3 Protocolo de Configuración de Hosts Dinámico

El DHCP[12] (Protocolo de Configuración de Hosts Dinámico) *se basa en el* RFC 2131, y trabaja en modo cliente – servidor. El protocolo de configuración de hosts dinámico, habilita a los clientes DHCP, obtener sus configuraciones desde un servidor DHCP, considerando que la opción de configuración de mayor importancia, es la dirección IP asignada al cliente.

Nota: El DHCP no se utiliza para la configuración de los switches, routers o servidores. Estos hosts necesitan tener direcciones estáticas.

DHCP usa el UDP[13] como protocolo de transporte. El cliente envía mensajes al servidor sobre el puerto 67, mientras que el servidor envía mensajes al cliente sobre el puerto 68. Los clientes DHCP arriendan la información del servidor por un periodo definido administrativamente. Y cuando el arrendamiento expira, el cliente debe pedir otra dirección, auque generalmente se le reasigna la misma.

2.1.3.1 Operación del DHCP

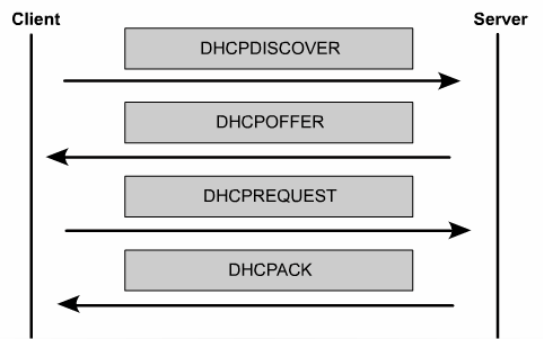


Figura 2.5 Orden de la Transmisión de Mensajes DHCP[14]

Nota: El cliente debe estar configurado para usar DHCP.

1. El cliente envía un *request* o pedido al servidor solicitando una configuración IP, lo cual lo realiza enviando un broadcast denominado DHCPDISCOVER dentro de la

[12] Dynamic Host Configuration Protocol
[13] User Datagram Protocol
[14] Figura de Cisco CCNA4, DHCP Operation

red local. El cliente muchas veces puede sugerir la dirección IP que desea, tal como cuando pide un incremento en el periodo de arrendamiento.

2. Una vez que el servidor recibe el broadcast, éste verifica si puede dar servicio al *request* desde su propia base de datos. Si no puede realizarlo, entonces envía el pedido a otro servidor DHCP, pero si lo puede hacer, el servidor DHCP ofrece la información de configuración IP al cliente en forma de un unicast DHCPOFFER. El DHCPOFFER es una configuración propuesta que puede incluir la dirección IP, la dirección del servidor DNS, y el tiempo de arrendamiento.
3. Si el cliente encuentra la oferta satisfactoria, este envía otro broadcast conocido como DHCPREQUEST, pidiendo específicamente los parámetros IP. La razón por la que el cliente envía otro broadcast en lugar de un unicast al servidor, es porque el primer *request*: DHCPDISCOVER pudo haber sido alcanzado por más de un servidor, y por ende fueron enviadas varias ofertas, por lo tanto el DHCPREQUEST les va a permitir conocer a los servidores que oferta fue aceptada. Generalmente la oferta aceptada es la primera en ser recibida.

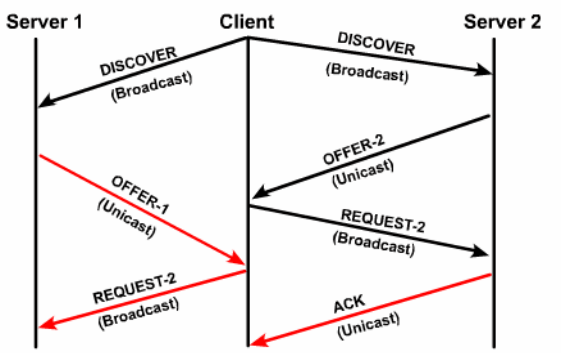


Figura 2.6 Operación del DHCP[15]

4. El servidor que recibe el DHCPREQUEST hace la configuración oficial enviando un acuse de recibo (*acknowledgment*) unicast, conocido como DHCPACK. La recepción del DHCPACK habilita al cliente a usar inmediatamente la dirección asignada. Si el servidor no envía el DHCPACK, lo cual es muy poco probable, es porque el servidor asigno esa información a otro cliente en el tiempo interino.
5. Si el cliente detecta que la dirección ya está en uso, el cliente envía un mensaje DHCPDECLINE y el proceso comienza de nuevo. Si el cliente recibe un

[15] Figura de Cisco CCNA4, DHCP Operation

DHCPNACK luego de ser enviado el DHCPREQUEST, el proceso también reinicia nuevamente.

6. Si el cliente no necesita la dirección IP, el cliente envía un mensaje DHCPRELEASE al servidor.

Dependiendo de las políticas de la organización, es posible asignar direcciones estáticas a hosts dentro del rango de direcciones del servidor DHCP. Ciertos servidores antes de realizar la oferta de la dirección IP, chequean que esta dirección no esté ocupada, publicando un ICMP *echo request* o haciendo ping al pool de direcciones, antes de enviar el DHCPOFFER al cliente.

En las siguientes gráficas se muestra la operación del DHCP.

DHCPDISCOVER:

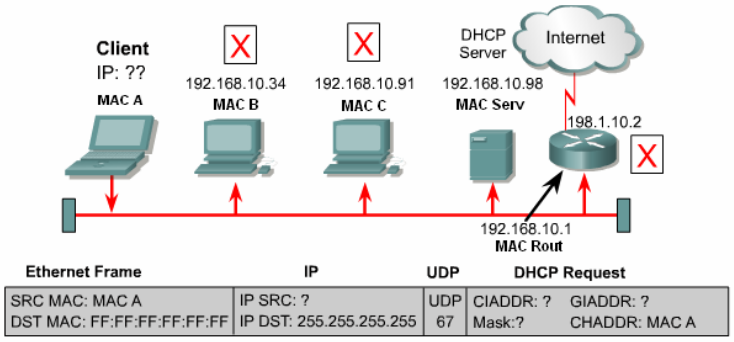


Figura 2.7 DHCPDISCOVER[16]

DHCPOFFER:

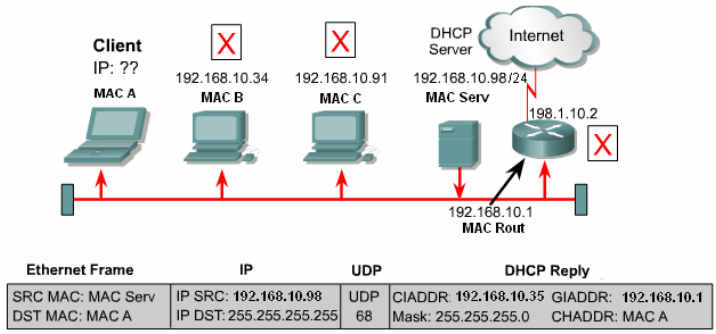


Figura 2.8 DHCPOFFER[17]

[16] Figura editada de Cisco CCNA1, DHCP IP address management
[17] Figura editada de Cisco CCNA1, DHCP IP address management

DHCPREQUEST:

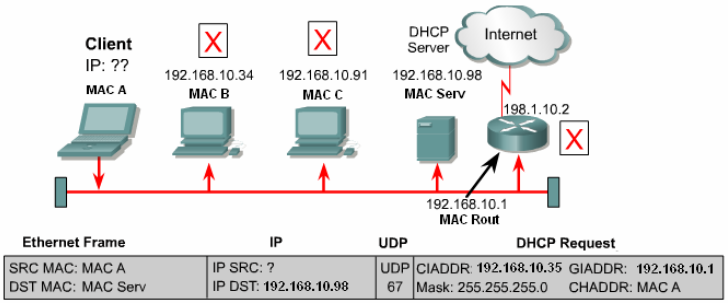


Figura 2.9 DHCPREQUEST[18]

DHCPACK:

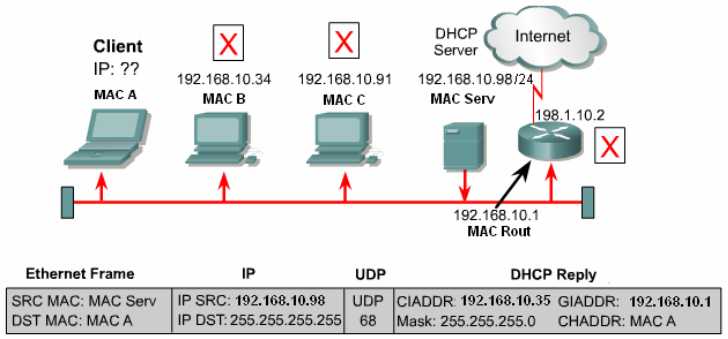


Figura 2.10 DHCPACK[19]

Estos son los significados de los campos que utiliza el paquete DHCP:

- CIADDR: Dirección IP del cliente (*Client IP Address*)
- GIADDR: Dirección IP del *Gateway*[20] (*Gateway IP Address*)
- CHADDR: Dirección del Hardware del cliente (*Client Hardware Address*)

2.1.3.2 DHCP Relay

Los clientes DHCP usan broadcast IP para encontrar al servidor DHCP sobre el mismo segmento. En el caso de no tener al servidor y a los clientes sobre el mismo segmento y separados por un router, que es un dispositivo que no envía los broadcast más allá de la subred, es necesario usar la característica *helper-address* de los propios dispositivos de capa 3, utilizando el comando **ip helper-address** para pasar los *request* broadcast de los clientes DHCP u otros servicios UDP, a una dirección IP específica, que sería la del servidor DHCP, vía unicast.

[18] Figura editada de Cisco CCNA1, DHCP IP address management
[19] Figura editada de Cisco CCNA1, DHCP IP address management
[20] Interface de un router por donde ingresa o sale el tráfico de una red local

El cliente realiza un broadcast del paquete DHCPDISCOVER sobre su segmento local. Este paquete es recogido por el *gateway* y si se encuentra configurado el *ip helper-address*, el paquete DHCP es enviado a la dirección específica configurada. El servidor llena el campo GIADDR con la dirección IP del *gateway* por el cual ingresó el *request* DHCP, dirección que luego será el *gateway* para los clientes DHCP. Además el *gateway* por el cual ingresa el *request* le indica al servidor DHCP de qué rango de direcciones se va a tomar la dirección IP para asignarle al cliente DHCP, debido a que pueden estar configurados varios pools de direcciones, pero con sus respectivos *gateways*.

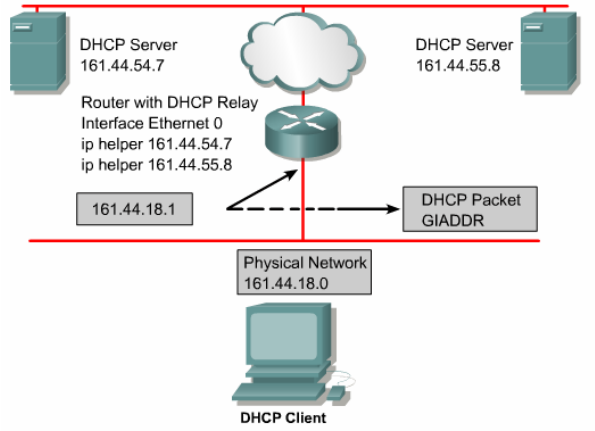


Figura 2.11 DHCP Relay con dos Servidores DHCP[21]

El DHCP relay puede ser configurado para enviar el paquete a varios servidores DHCP. El cliente elige el "mejor" servidor.

La Figura 2.12 muestra el *request* que realiza un cliente DHCP desde una red diferente a la que se encuentra el servidor DHCP.

[21] Figura de Cisco CCNA4, DHCP Relay

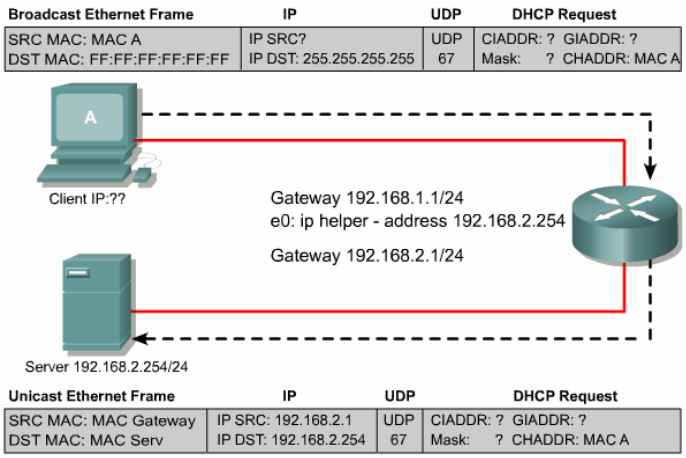


Figura 2.12 Pedido DHCP usando DHCP Relay[22]

En la siguiente figura se muestra la respuesta del servidor DHCP, a la petición del cliente DHCP.

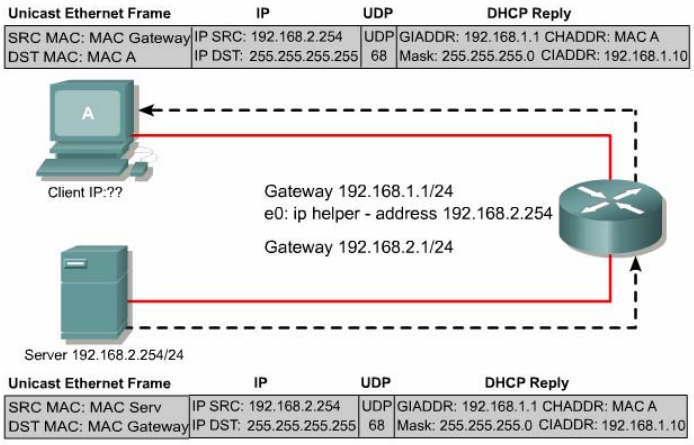


Figura 2.13 Respuesta DHCP usando DHCP Relay[23]

Por defecto el comando ip helper-address envía los siguientes servicios UDP:

- Time
- TACACS
- DNS
- BOOTP/DHCP Server
- BOOTP/DHCP Client
- TFTP
- NetBIOS Name Service
- NetBIOS datagram Service

[22] Figura de Cisco CCNA4, DHCP Relay
[23] Figura editada de Cisco CCNA4, DHCP Relay

2.1.3.3 Secuencia de Inicio de los Teléfonos IP Mitel con el DHCP Mitel

Esta es la normal secuencia de eventos para un teléfono IP dual port, donde VLANs son implementadas:

- Encendido.
- Corre el 'Boot' code.
- Solicita la dirección IP (no etiquetado) a través de DHCP
- Recibe la dirección IP sobre la VLAN nativa (VLAN de datos) y opciones de sistema.
- Comprueba la información VLAN.
- Abandona la dirección IP (no etiquetada).
- Solicita la dirección IP sobre la VLAN de voz (etiquetada).
- Recibe la dirección IP sobre la VLAN de voz y opciones del sistema, otra vez.
- Chequea que la información VLAN coincida, y si no se repite hasta que esto ocurra.
- Localiza el servidor TFTP.
- Obtiene el *running code.*
- Se registra con el control de llamada.
- OK

2.1.4 Ethernet

Ethernet o su estándar equivalente IEEE 802.3, es básicamente una tecnología de transmisión broadcast, donde los dispositivos como computadoras, impresoras, servidores de archivos, etc.; se comunican sobre un medio de transmisión compartido, lo que quiere decir que ellos se encuentran en una continua competencia por el ancho de banda disponible. Por lo tanto las colisiones son una natural ocurrencia en redes Ethernet y pueden llegar a ser un gran problema.

La entrega de tramas de datos Ethernet es de de naturaleza broadcast. Ethernet usa el método CSMA/CD[24] (Acceso Múltiple Sensible a Portadora con Detección de Colisión), que le permite a una sola estación transmitir, y puede soportar tazas de transmisión de alta

[24] Carrier Sense Multiple Access / Collision Detection

velocidad, como: Ethernet: 10 Mbps, Fast Ethernet: 100 Mbps, Gigabit Ethernet: 1000 Mbps y 10-Gigabit Ethernet: 10,000 Mbps.

El desempeño de un medio compartido Ethernet/802.3 puede ser negativamente afectado por factores como: las aplicaciones multimedia con alta demanda de ancho de banda tales como video e Internet, que junto con la naturaleza broadcast de Ethernet, pueden crear congestión en la red; y la latencia normal que adquieren las tramas por viajar a través de los medios de red, atravesar dispositivos de red y los propios retardos de las NICs.

2.1.5 Dominio de Colisión

Es un grupo de dispositivos conectados al mismo medio físico, es decir si dos dispositivos acceden al mismo tiempo al medio, entonces esto resulta en una colisión. Este es un dominio de capa 1.

2.1.6 Dominio de Broadcast

Es un grupo de dispositivos sobre la red que reciben mensajes de broadcast. Este es un dominio de capa 2.

2.1.7 Broadcast y Multicast

Para comunicarse con todos los dominios de colisión, los protocolos usan tramas broadcast y multicast en la capa 2 del modelo OSI. Por lo tanto si un nodo necesita comunicarse con todos los hosts en la red, éste envía una trama broadcast con una dirección MAC de destino 0xFFFFFFFFFFFF. Esta es una dirección a la cual todas las tarjetas NIC deben responder.

La acumulación de tráfico broadcast y multicast de cada dispositivo de la red es referido como: **radiación de broadcast,** cuya circulación puede saturar la red, es decir que no hay ancho de banda disponible para aplicaciones de datos, resultando en la caída de estas conexiones, situación conocida como una **tormenta de broadcast.**

2.1.7.1 Causas de Broadcast y Multicast

Existen varias fuentes de broadcast y multicast en redes IP, estas pueden ser: las estaciones de trabajo, los routers, las aplicaciones multicast, el protocolo DHCP, etc.

Las estaciones de trabajo envían broadcast de pedidos ARP[25] (Protocolo de Resolución de Direcciones), cada vez que ellos necesitan localizar una dirección MAC que no está en su tabla ARP. Las tormentas de broadcast pueden ser causadas por el pedido de información de un dispositivo dentro de una red que ha crecido mucho. Es decir muchas respuestas pueden ser causadas por el pedido original que el dispositivo no puede procesar, o el primer pedido activa similares pedidos de otros dispositivos que efectivamente bloquean el normal flujo de tráfico en la red.

Los protocolos de enrutamiento que están configurados en la red pueden también incrementar el tráfico broadcast significativamente, por ejemplo el protocolo RIP[26] usa los broadcast para retransmitir cada 30 segundos las tablas de enrutamiento entre los routers.

Las aplicaciones multicast, particularmente las aplicaciones de paquetes de video pueden generar una cadena de siete megabytes de datos multicast, que en una red conmutada podría ser enviada a cada segmento, resultando en una severa congestión.

Otra fuente generadora de broadcast es el protocolo DHCP, cuando un cliente DHCP usa un pedido de broadcast para localizar el servidor DHCP. Además estos clientes por lo general repiten este pedido después de un relativo corto “timeout”, posiblemente debido a una respuesta lenta del servidor, lo que producen las conocidas **tormentas de broadcast;** que a su vez producen retardos anormales de otros tráficos cliente / servidor, los cuales también pueden empezar a retransmitir.

[25] Address Resolution Protocol
[26] Routing Information Protocol

2.2 MODELO JERARQUICO CISCO

Consta de tres capas, (ver Figura 2.14):

- Capa Núcleo[27]: Backbone
- Capa de Distribución: Routing
- Capa de Acceso: Switching

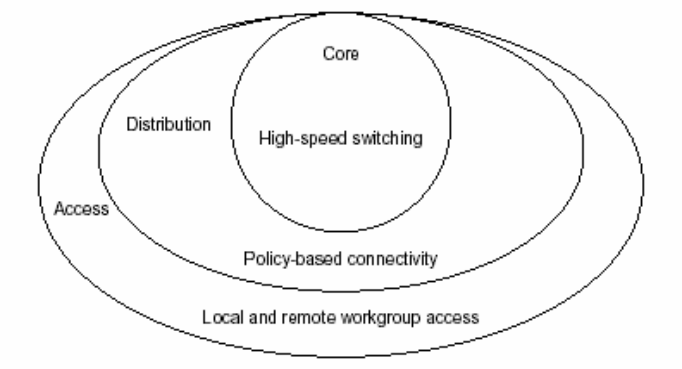


Figura 2.14 Capas del Modelo Jerárquico Cisco[28]

2.2.1 Capa Núcleo

Es el backbone de conmutación de alta velocidad que debe ser diseñado para conmutar paquetes lo más rápido posible, es decir es responsable del transporte de grandes cantidades de tráfico en forma confiable y rápida, por lo tanto la preocupación de esta capa es la velocidad y latencia.

Es importante considerar, lo que no debemos hacer en esta capa:

- No realizar ningún tipo de manipulación de paquetes, tal como usar listas de control de acceso, enrutamiento entre redes de área local virtuales (VLAN) o filtro de paquetes, lo cual reducirá el tráfico.
- No soporta accesos de grupo de trabajo.
- Evitar expandir el núcleo o *core* cuando la red crece. Si el desempeño es un problema en el *core*, son preferibles las actualizaciones en lugar de las expansiones.

[27] Core Layer
[28] Figura de Internetworking Design Basics, Chapter 2.

Ahora, lo que debemos considerar para diseñar la capa núcleo es:

- Diseñar el *core* para alta confiabilidad. Considerar las tecnologías de enlace de datos que facilitan tanto la velocidad como la redundancia, tales como: FDDI, Frame Relay, ATM[29], etc.
- Diseñar con la velocidad en mente. El *core* debe tener una muy pequeña latencia.
- Seleccionar protocolos de enrutamiento con tiempo de convergencia bajos. La conectividad de enlace de datos rápidos y redundantes no es una ayuda si tenemos tablas de enrutamiento disparadas.

2.2.2 Capa de Distribución

También conocida como "*workgroup layer"*, y es el punto de comunicación entre la capa de acceso y el *core*. Las principales funciones de la capa de distribución son el proveer enrutamiento, filtros, accesos WAN y determinar como los paquetes pueden acceder al *core* si es necesario.

La capa de distribución es donde se implementan las políticas para la red. Existen algunas acciones que generalmente deben hacerse en esta capa:

- Enrutamiento
- Implementación de listas de control de acceso o filtro de paquetes.
- Implementación de seguridad y políticas de red, incluyendo traslado de direcciones y firewalls[30].
- Calidad de Servicio, en base a las políticas definidas.
- Redistribución entre protocolos de enrutamiento, incluyendo rutas estáticas.
- Enrutamiento entre VLANs y otras funciones que soportan los grupos de trabajo.
- Definición de dominios de broadcast y multicast.
- Posible punto para acceso remoto.
- Traslado de medios de comunicación.

[29] Asyncronous Transfer Mode
[30] Sistema diseñado para prevenir el acceso no autorizado a o desde una red privada

2.2.3 Capa de Acceso

La capa de acceso es el punto en el cual los usuarios finales son conectados a la red. Esta capa puede también usar listas de acceso o filtros para optimizar las necesidades de un grupo particular de usuarios. Los recursos de red de la mayoría de usuarios deben estar disponibles localmente. Esta capa también es conocida como "*desktop layer*". Estas son algunas de las funciones que incluye esta capa:

- Continúa el control de acceso y políticas (desde la capa de distribución)
- Creación de dominios de colisión separados (micro-segmentación)
- Conectividad de los grupos de trabajo dentro de la capa de distribución.
- Habilitar filtros de direcciones MAC
- También es posible tener acceso a grupos de trabajo remotos.
- Presta servicios de asignación de VLANs a nivel de capa 2 del modelo OSI.

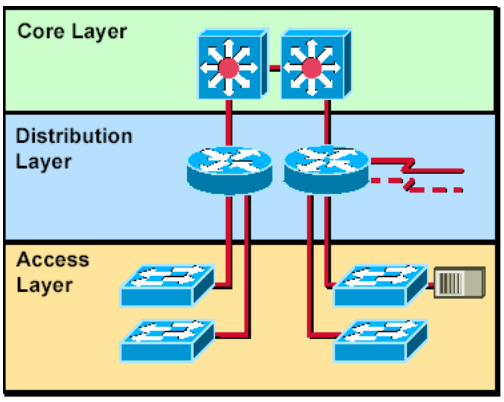


Figura 2.15 Estructura de Red definido por Jerarquía[31]

Nota: Cuando se realiza la implementación, podemos tener varios dispositivos en una sola capa, o podemos tener un solo dispositivo desarrollando funciones en varias capas. Es decir las 3 capas no necesariamente deben existir en distintas entidades físicas.

[31] Figura de Interconnecting Cisco Network Devices, Student Guide.

2.3 RED DE AREA LOCAL VIRTUAL

Una VLAN[32] (Red de Area Local Virtual) es una agrupación lógica de dispositivos o servicios de red, en base a funciones, departamentos, equipos de trabajo o aplicaciones, sin considerar la localización física o conexiones de red. Ver Figura 2.16.

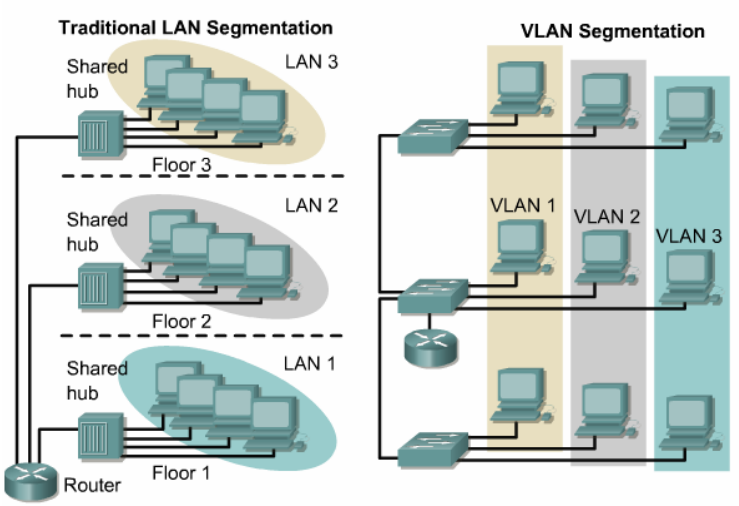


Figura 2.16 VLANs y Límites Físicos[33]

La función de las VLANs es una segmentación lógica de la red en diferentes dominios de broadcast, es decir que los paquetes son solamente conmutados entre puertos que han sido asignados a la misma VLAN. Por lo tanto los dispositivos sobre una VLAN solo pueden comunicarse con los dispositivos que pertenecen a la misma VLAN, porque cada una de ellas es un dominio de broadcast diferente.

Así como solo los routers proveen conectividad entre diferentes segmentos LAN, también solo los routers o equipos que operen en la capa tres del modelo OSI, proveen conectividad entre diferentes segmentos VLAN. Los routers en topologías VLAN proveen filtrado de broadcast, seguridad y administración del flujo de tráfico.

Las VLANs consisten de hosts o equipos de red conectados por un solo dominio de bridging. Los switches LAN trabajan con protocolos bridging con un grupo de bridge por separado por cada VLAN. Los switches no puentean (not bridge) el tráfico entre VLANs porque esto violaría la integridad del dominio de broadcast VLAN; el tráfico solamente puede ser enrutado entre VLANs.

[32] Figura de Cisco CCNA3, VLAN Introduction

Las VLANs son creadas para proveer segmentación de servicios tradicionalmente dado por los routers en las configuraciones LAN, es decir las VLANs representan una solución alternativa a los routers con función de gestores de red.

Las VLANs operan en la capa 2 y 3 del modelo OSI.

2.3.1 Beneficios de las VLANs

- Incrementan el desempeño de la red agrupando estaciones de trabajo, recursos y servidores según su función, sin importar si ellos se encuentran en el mismo segmento físico LAN.**(Mejor desempeño, Facilidad de Administración).**
- Facilidad en la administración de adición, movimiento y cambio de estaciones de trabajo en la red.**(Flexibilidad, Escalabilidad, Facilidad de Administración).**
- Mejoran la seguridad de la red, porque solamente las estaciones de trabajo que pertenezcan a la misma VLAN podrán comunicarse directamente (sin enrutamiento). **(Seguridad).**
- Incrementan el número de dominios de broadcast mientras éstos decrecen en su tamaño. **(Mejor desempeño)**.
- Facilitan el control de flujo de tráfico, porque permiten controlar la cantidad y tamaño de los dominios de broadcast, debido a que éstos por defecto son filtrados desde todos los puertos que no son miembros de la misma VLAN en un switch.**(Mejor desempeño).**
- La configuración o reconfiguración de VLANs se realiza a través de software, por lo tanto esto no requiere de movimientos o conexiones físicas de los equipos de red. **(Facilidad de Administración).**

En conclusión las VLANs proveen flexibilidad, escalabilidad, seguridad, facilidad de administración y mejor desempeño de la red

El comportamiento de un Switch con VLANs es el siguiente:

- El switch tiene una tabla de bridging separada por cada VLAN.

- Si la trama llega a un puerto de cierta VLAN, el switch busca la tabla de bridging solo de esa VLAN.
- Cuando una trama es recibida, el switch añade la dirección de origen a la tabla de bridging, si ésta no es conocida.
- El destino es chequeado para que la decisión de envío sea realizada.

2.3.2 Tipos de asignación a VLANs

Cada puerto de un switch puede ser asignado a una VLAN diferente. Los puertos asignados a la misma VLAN comparten broadcasts, mientras que los puertos que no pertenecen a esa VLAN no comparten estos broadcasts. Esto mejora el comportamiento global de la red.

En forma general existen dos formas de asignación a VLANs, y estas son:

- VLANs Estáticas, y
- VLANs Dinámicas

2.3.2.1 VLANs Estáticas

También llamadas, VLANs basadas en puertos o VLANs de puerto-céntrico

VLANs en base a puertos

Consiste, en que cada puerto de un switch es asignado a una VLAN. Por lo tanto, el dispositivo que se conecte a cualquier puerto pertenecerá automáticamente a la VLAN asignada a ese punto.

Cuando se usa este tipo de asignación, todos los usuarios del mismo puerto estarán en la misma VLAN, ya sea uno o varios usuarios al mismo tiempo (utilizando un HUB).

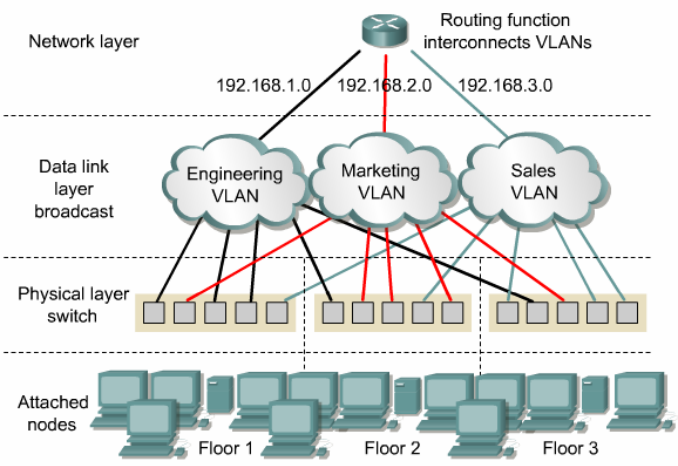


Figura 2.17 VLANs en base a Puertos[34]

Características:

- Es la forma más usual de crear VLANs.
- El administrador de red debe configurar puerto a puerto las VLANs.
- Las VLANs estáticas son las más seguras, fácil de configurar y monitorear.
- Trabaja bien donde el movimiento de usuarios dentro de una red es controlado.
- El administrador de red debe reconfigurar los puertos de los switches cada vez que el usuario se mueve de un lugar a otro (cambia de puertos).
- No utiliza tablas de búsqueda (lookup) para segmentar las VLANs

La VLAN por defecto para cada puerto en un switch es la VLAN de administración o gestión, que siempre es la VLAN 1 y no puede ser borrada. La configuración de los switches sólo puede realizar desde la VLAN de gestión.

2.3.2.2 VLANs Dinámicas

La pertenencia de estaciones de trabajo a cada VLAN es en base a sus direcciones MAC (capa 2), direcciones lógicas (capa 3) o en base a reglas y políticas.

a) VLANs en base a Direcciones MAC

Operan agrupando estaciones finales a una VLAN en base a sus direcciones MAC. La forma en como se realiza la asignación de usuarios a una VLAN es utilizando un

[34] Figura de Cisco CCNA3, VLAN Operation

servidor de políticas de administración de VLANs (VMPS[35]), para que maneje la base de datos de todas las direcciones MAC; de tal forma que cuando un usuario se conecte a un puerto de un switch, éste último, consulte al servidor a que VLAN corresponde este dispositivo, de acuerdo a su dirección MAC.

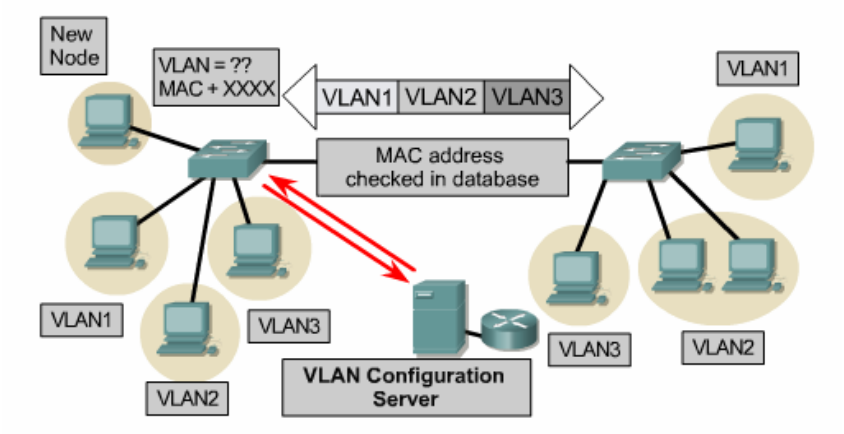


Figura 2.18 VLANs en base a Direcciones MAC[36]

Permite a los administradores de red mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. Por lo tanto las VLANs basadas en MAC prestan su mayor servicio de movilidad y seguridad a nivel de computadoras portátiles.

La principal desventaja, es que inicialmente se necesita recopilar la información de las direcciones MAC de todas las estaciones de trabajo de la red, para construir la base de datos que necesita el servidor de políticas VLAN. Lo cual será un gran inconveniente si estamos trabajando con redes grandes. Después de esa configuración inicial, ahora sí el movimiento automático de usuarios es posible.

Características:

- Necesita un servidor de políticas de administración VLANs (VMPS).
- No necesita administración al realizar desplazamientos de usuarios.
- Notificación cuando un usuario desconocido quiere ingresar a la red.
- Un usuario no puede conectarse a la red sin la aprobación del administrador.

[35] VLAN Management Policy Server
[36] Figura de Cisco CCNA3, VLAN Operation

- Inconveniente en levantar la base de datos inicial de direcciones MAC de una red grande.
- Raramente implementado hoy en día
- Para los usuarios es muy útil.
- Dificultad en la administración y para resolver problemas
- Ofrece flexibilidad, pero a pesar de eso se añaden cabeceras.
- Impacta en el desempeño, escalabilidad y administración de la red.

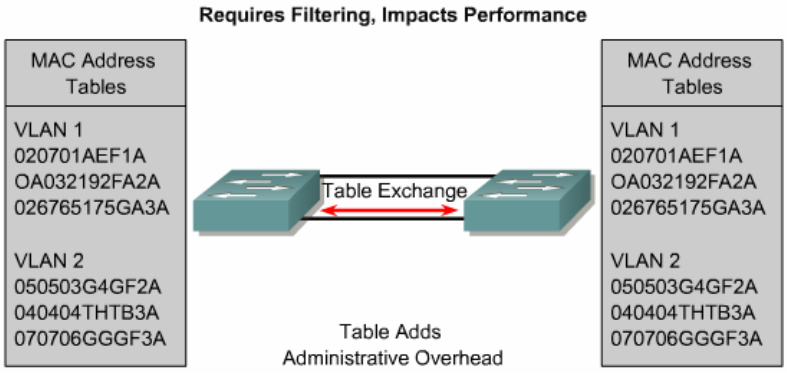


Figura 2.19 Membresía por Direcciones MAC[37]

Servidor de políticas de administración VLAN (VMPS)

Con el servidor VMPS, se asignan dinámicamente los puertos de los switches a VLANs que están basadas en la dirección MAC del dispositivo conectado al puerto.

Como trabaja VMPS:

Cuando se habilita el VMPS, la base de datos de las direcciones MAC con sus respectivas VLANs es descargada de un servidor TFTP[38] al servidor VMPS, y el servidor VMPS empieza a aceptar los pedidos (*requests*) de los clientes. VMPS permanece habilitado, sin considerar si se resetea o "*power cycle*" el switch.

El VMPS abre un *socket* UDP para comunicarse y escuchar los pedidos de los clientes. Cuando el servidor VMPS recibe un pedido válido de un cliente, éste busca en su base de datos la VLAN que le corresponde a la dirección MAC.

[37] Figura de Cisco CCNA3, VLAN Types
[38] Trivial File Transfer Protocolo

"Si la VLAN asignada es restringida a un grupo de puertos, el servidor VMPS verifica el puerto que hace el pedido, con éste grupo. Si la VLAN es permitida sobre el puerto, el nombre de la VLAN es retornada al cliente. Si la VLAN no es permitida sobre el puerto y el servidor VMPS está en ***modo abierto*** "*open mode*", el host recibe la respuesta "access denied". Si el servidor VMPS esta en ***modo seguro*** "*secure mode*" el puerto es deshabilitado ("*shut down*") y se debe manualmente traer el respaldo del puerto con el comando ***set port*"[39].**

Si ninguna dirección MAC de la base de datos del servidor VMPS, no corresponde con la dirección MAC presente en el puerto. VMPS envía una respuesta de acceso denegado en modo abierto o deshabilitar el puerto si el servidor está en modo seguro.

VLAN de respaldo (Fallback VLAN)

Una característica importante que soportan las VLANs dinámicas y más explícitamente al servidor VMPS, es la VLAN de respaldo, que permite automáticamente configurar a un puerto a una VLAN especialmente creada para estaciones cuyas direcciones MAC no están en el servidor VMPS. Es decir el servidor VMPS enviará el nombre de la VLAN de *Fallback* cuando éste no encuentre en la base de datos la dirección MAC del dispositivo conectado a cierto puerto.

Si no se configura una VLAN de *Fallback* y la dirección MAC no existe en la base de datos, VMPS envía una respuesta de acceso denegado en modo abierto, o la respuesta de deshabilitar el puerto en modo seguro.

Por ejemplo se puede utilizar para los visitantes o clientes de una empresa, que requieren de un acceso restringido y específico a la red, ellos se pueden conectar libremente a la red y tener acceso a Internet, pero con derechos limitados a directorios públicos.

[39] Configuring Dinamic VLAN Membership with VMPS, Chapter 12, Switch 4500 Series.

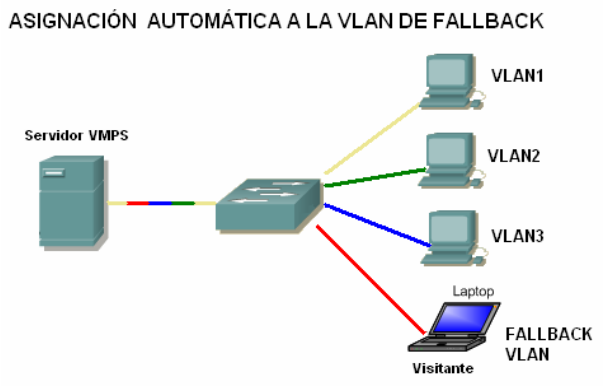


Figura 2.20 Asignación Automática a la VLAN de Fallback

Además se puede crear una entrada explícita en la tabla de configuración, para denegar el acceso a direcciones MAC específicas por razones de seguridad, especificando la palabra **"NONE"** en el nombre de la VLAN. En este caso, VMPS envía una respuesta de acceso denegado o de deshabilitar el puerto, dependiendo en que modo esté operando el VMPS.

Un puerto dinámico puede pertenecer solamente a una *VLAN nativa* en publicaciones de software anteriores a la 6.2(1). Con la publicación de software 6.2(1), un puerto puede pertenecer a una VLAN nativa y a una VLAN auxiliar, que se utiliza generalmente para los teléfonos IP.

Una de las restricciones, cuando se conectan varias estaciones de trabajo a un mismo puerto con asignación dinámica de VLANs, utilizando un dispositivo de medio compartido como un HUB, es que todas estas estaciones de trabajo deben estar configuradas en el servidor VMPS como parte de la misma VLAN, de lo contrario el puerto es deshabilitado o sus accesos son denegados como una medida de seguridad, ver Figura 2.21. Además un puerto dinámico puede usar hasta 50 hosts activos (direcciones MAC), si todos ellos son autorizados en la misma VLAN, de lo contrario éste puerto será deshabilitado o sus accesos son denegados.

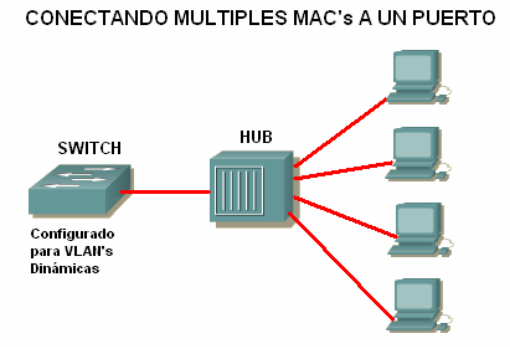


Figura 2.21 Conectando Múltiples MACs a un Puerto

Si se mueve un host desde un puerto dinámico a otro, el puerto permanece asignado a la VLAN, hasta que otra dirección MAC cambie la VLAN.

b) VLANs en base a Capa 3

Las VLANs de capa 3 toman en cuenta el **tipo de protocolo** (si varios protocolos son soportados por la máquina) o **direcciones de la capa de red**, para determinar la pertenencia a una VLAN.

Si se configura específicamente por el tipo de protocolo, un ejemplo es, lo que pertenezca a IP sé enrutará a la VLAN de IP e IPX se dirigirá a la VLAN de IPX.

Hay varias ventajas en definir VLANs de capa 3. En primer lugar, permite el particionado por tipo de protocolo, lo que puede parecer atractivo para los administradores que están dedicados a una estrategia de VLAN basada en servicios o aplicaciones. En segundo lugar, los usuarios pueden físicamente mover sus estaciones de trabajo sin tener que reconfigurar cada una de las direcciones de red de la estación (este es un beneficio principalmente para los usuarios de TCP/IP).

Una de las desventajas de definir la VLAN de capa 3 es su modo de trabajo. El inspeccionar direcciones de la capa 3 en paquetes consume más tiempo que buscar una dirección MAC en tramas.

Las VLANs basadas en capa 3 son particularmente efectivas en el trato con TCP/IP, pero mucho menos efectivas con protocolos como IPX, DEC*net* o *AppleTalk*, que no implican configuración manual. Además tienen la dificultad al tratar con protocolos no

enrutables como NetBIOS (estaciones finales que soportan protocolos no enrutables no pueden ser diferenciadas y, por tanto, no pueden ser definidas como parte de una VLAN).

El uso de VLANs basadas en direcciones de red no es muy común, porque generalmente las redes usan servidores DHCP para asignar dinámicamente las direcciones IP de los hosts, lo cual implica que no es conviene utilizar éste método.

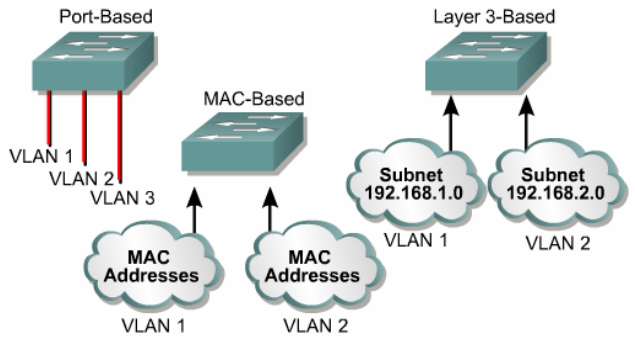


Figura 2.22 Establecimiento de Membrecía VLAN[40]

2.3.3 Fundamentos de VLANs

El **número de VLANs** en un switch, varia dependiendo de algunos factores:

- Patrones de tráfico
- Tipos de aplicación
- Necesidades de administración de red
- Grupos de trabajo

El esquema de direccionamiento es otra importante consideración en la definición del número de VLANs en un switch.

Cada VLAN debe tener una única dirección de capa 3 asignada. Esto permite a los routers conmutar paquetes entre VLANs.

Las VLANs pueden existir en redes extremo a extremo o dentro de fronteras geográficas.

[40] Figura de Cisco CCNA3, VLAN Types

2.3.3.1 VLANs Extremo a Extremo[41]

Comprende de las siguientes características:

- La afiliación de usuarios a cada VLAN es en base al departamento o función de trabajo, sin considerar donde los usuarios están localizados.
- Todos los usuarios en una VLAN deben tener el mismo **patrón de flujo de tráfico 80/20**.
- La agrupación de usuarios a cada VLAN no debe cambiar cuando ellos son reubicados dentro del campus.
- Cada VLAN tiene un conjunto de requerimientos de seguridad para todos los miembros.

En la Figura 2.23, los servidores de grupo de trabajo operan en el modelo cliente/servidor. Por esta razón, los usuarios son asignados a la misma VLAN con el servidor que ellos utilicen, y así maximizar el desempeño de la conmutación de capa 2 y mantener localizado el tráfico. Es decir la VLAN extremo a extremo permite a los dispositivos ser agrupados en base al uso de recursos.

La red es diseñada en base al patrón de flujo de tráfico, para tener un 80 por ciento del tráfico contenido dentro de la VLAN, y el restante 20 por ciento que cruce el router para tener acceso a servidores de la empresa, al internet y a la WAN. Ver Figura 2.23.

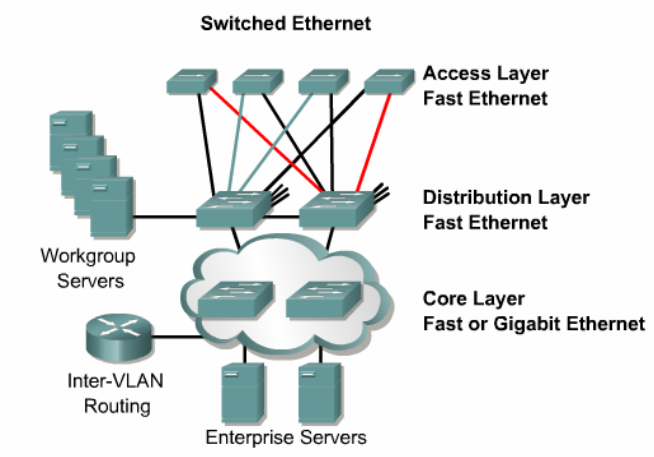


Figura 2.23 VLANs Extremo a Extremo[42]

[41] End-to-End VLANs
[42] Figura de Cisco CCNA3, VLAN basics

2.3.3.2 VLANs Geográficas

Cuando redes corporativas tienden a centralizar sus recursos, las VLANs extremo a extremo (80/20), llegan a ser difícil de mantener. Los usuarios utilizan diferentes recursos, muchos de los cuales no se encuentran en su propia VLAN. Este cambio en el uso de recursos requiere que las VLANs sean creadas alrededor de fronteras geográficas en lugar de fronteras comunes.

Esta localización geográfica puede ser tan grande como un edificio entero o tan pequeño como un simple switch dentro de un armario. En una estructura de VLAN geográfica, es típico encontrar la nueva regla 20/80 en efecto. Esto significa que el 20 por ciento del tráfico se mantiene dentro de la VLAN local y el 80 por ciento del tráfico de la red viaja fuera de la VLAN local. Aunque esta topología significa que el 80 por ciento de los servicios de los recursos deben viajar a través de un dispositivo de capa 3, éste diseño permite a las redes proveer un método determinístico y consistente para acceder a los recursos.

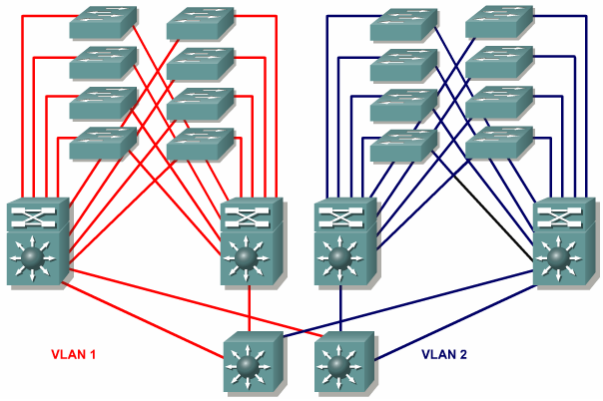


Figura 2.24 VLANs Geográficas[43]

2.3.4 Transporte de VLANs

Las tramas son manejadas por los switches en forma diferente de acuerdo al tipo de enlace que ellas están atravesando. Existen dos tipos de enlaces diferentes en un medio conmutado (utilizan switches).

[43] Figura de Cisco CCNA3, Geographic VLANs

2.3.4.1 Enlaces de Acceso

Estos enlaces le permiten a las estaciones de trabajo ganar acceso a la red. Este tipo de enlace solamente forma parte de una VLAN, y es conocida como VLAN *nativa* del puerto. Los switches eliminan cualquier información de VLAN de las tramas antes de ser enviadas a cualquier dispositivo ligado a un enlace de acceso. Ver Figura 2.25.

Los dispositivos de un enlace de acceso no pueden comunicarse con dispositivos fuera de su VLAN a menos que el paquete sea enrutado.

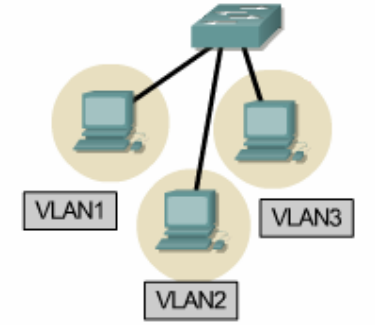


Figura 2.25 Enlaces de Acceso

Es importante notar que cualquier dispositivo conectado a un enlace de acceso es totalmente inconsciente de la VLAN asignada al puerto, simplemente asume que es parte de un dominio de broadcast.

Si un puerto de acceso recibe un paquete etiquetado (ISL o 802.1Q) con la VLAN asignada al puerto, el paquete es enviado; pero si se recibe un paquete etiquetado para otra VLAN, el paquete es desechado, la dirección fuente no es aprendida, y la trama es contabilizada en la estadística "*no destination*".

Dos tipos de puertos de acceso son soportados:

- Puertos de acceso estático, manualmente asignados a una VLAN.
- Puertos de acceso dinámico en la membresía VLAN, a través de paquetes entrantes.

Generalmente estos enlaces son de 10 o 100 Mbps.

2.3.4.2 Enlaces Troncales

Su nombre originalmente proviene de tecnologías de telefonía y radio, donde las troncales del sistema telefónico transportan múltiples conversaciones telefónicas, y las troncales de radio son líneas de comunicación simple que llevan varias señales de radio.

Actualmente este principio de troncales es aplicado a tecnologías de conmutación de redes. Una troncal es una conexión física y lógica entre dos switches, entre un switch y un router, o entre un switch y un servidor (con una NIC especial que soporte *trunking*), a través del cual el tráfico de red viaja. Generalmente es un enlace punto a punto de 100 o 1000 Mbps. Es decir los puertos FastEthernet de un switch son configurable porque pueden funcionar para enlaces de acceso o enlaces troncales.

El propósito de las troncales es evitar poner un enlace por cada VLAN, como se muestra en la Figura 2.26. Esta es una simple forma de implementar la comunicación de VLANs entre switches, pero esta no es escalable.

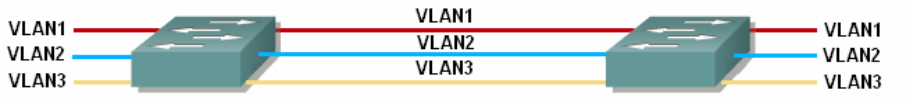


Figura 2.26 Un enlace por VLAN

Las troncales llevan el tráfico de múltiples VLANs sobre un solo enlace físico, desde 1 a 1005 al mismo tiempo, ver Figura 2.27.

Figura 2.27 Enlace Troncal con Múltiples VLANs

Es importante entender que un enlace troncal no pertenece a ninguna VLAN específica. Simplemente es un conducto para VLANs entre switches y routers.

Las troncales permiten convertir a un simple puerto, en parte de múltiples VLANs al mismo tiempo. Lo cual es una verdadera ventaja, por ejemplo, actualmente se puede configurar para tener un servidor en varios dominios de broadcast simultáneamente, lo que

quiere decir que usuarios de diferentes dominios de broadcast no necesitarán cruzar un dispositivo de capa 3 (router) para acceder al mismo servidor. Otro beneficio de las troncales, es cuando conectamos switches, y éstas nos permiten llevar algo o toda la información de las VLANs a lo largo del enlace, pero si estos enlaces entre los switches no son troncalizados, solamente la información de la VLAN 1 será conmutada a través del enlace por omisión.

Operación del Trunking

Los protocolos de *trunking* fueron desarrollados para eficazmente manejar la transferencia de tramas desde diferentes VLANs sobre una sola línea física. Estos protocolos establecen un acuerdo para la distribución de tramas hacia los puertos asociados, en ambos extremos de la troncal.

Existen dos tipos de mecanismos o protocolos de *trunking*, es decir dos formas de cómo se transmite la **información acerca de la pertenencia de los usuarios a las distintas VLANs** a través del backbone**:**

- Filtrado de tramas
- Etiquetado de tramas

a) Trunking con filtrado de tramas

Las tablas de filtrado son creadas por cada switch, asociando cada dirección física con la VLAN a la que pertenece. Los switches comparten estas tablas a través del backbone. Por lo tanto cuando llega una trama a un switch, las tablas de conmutación en los dos extremos de la troncal son usadas para realizar las decisiones de envío basadas en las direcciones MAC de destino de las tramas. Ver Figura 2.28.

A medida que el número de VLANs que viajan a través de la troncal se incrementa, las decisiones de envío llegan a ser más lentas y más difícil de manejar. Es decir el proceso de decisión se hace lento porque toma tiempo procesar las tablas de conmutación más grandes. Estas son razones por las cuales no se emplea actualmente este tipo de *trunking*.

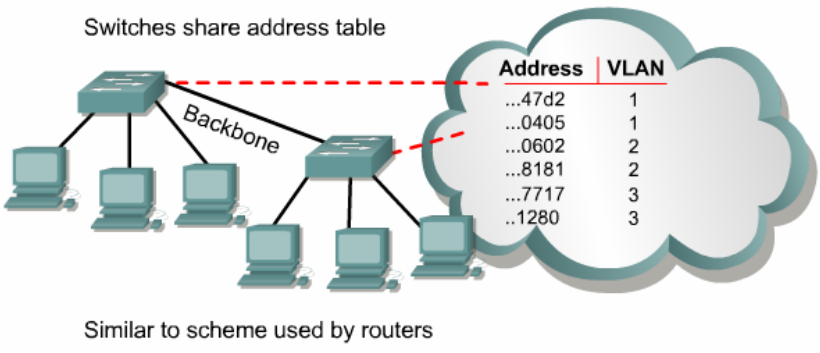


Figura 2.28 Filtrado de Tramas[44]

b) Trunking con etiquetado de tramas

Este método tiene asociado un identificador para cada VLAN, algunas personas se refieren a esto como el "VLAN ID" o "color".

Las tramas procedentes de los usuarios, antes de ser enviadas a través del enlace troncal o backbone, se etiquetan con el identificador correspondiente a la VLAN a la que pertenecen. Este identificador es entendido y examinado por cada switch antes de cualquier broadcast o transmisión a otros switches, routers o estaciones de trabajo. Una vez que la trama va a abandonar el backbone, entonces el switch elimina el identificador antes de ser enviada a la estación final. Ver Figura 2.29.

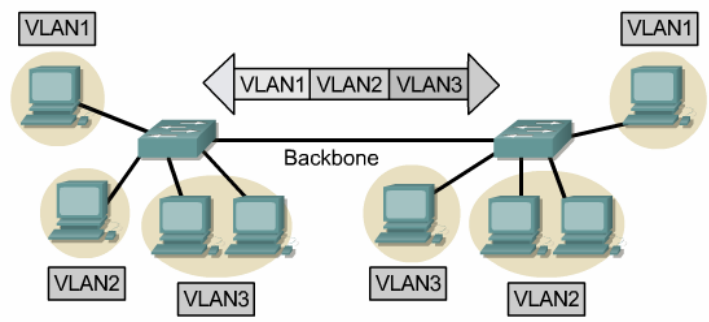


Figura 2.29 Etiquetado de Tramas[45]

En conclusión, los protocolos de *trunking* que usan etiquetamiento, consiguen la entrega de tramas en forma más rápida y hacen su manejo más fácil.

[44] Figura de Cisco CCNA3, Trunking Operation
[45] Figura de Cisco CCNA3, Trunking Operation

2.3.4.3 Tipos de Etiquetamiento

Existen diferentes esquemas de etiquetamiento, entre ellos tenemos:

- LAN *Emulation*
- 802.10 (FDDI)
- Inter-Switch Link (ISL)
- IEEE 802.1Q

Pero, los esquemas más comunes para etiquetamiento de segmentos Ethernet son ISL e IEEE 802.1Q.

2.3.4.3.1 LAN Emulation (LANE)

Fue introducida para resolver la necesidad de crear VLANs sobre enlaces WAN. Es decir esta tecnología nos permite crear oficinas remotas sin considerar su localización y distancia.

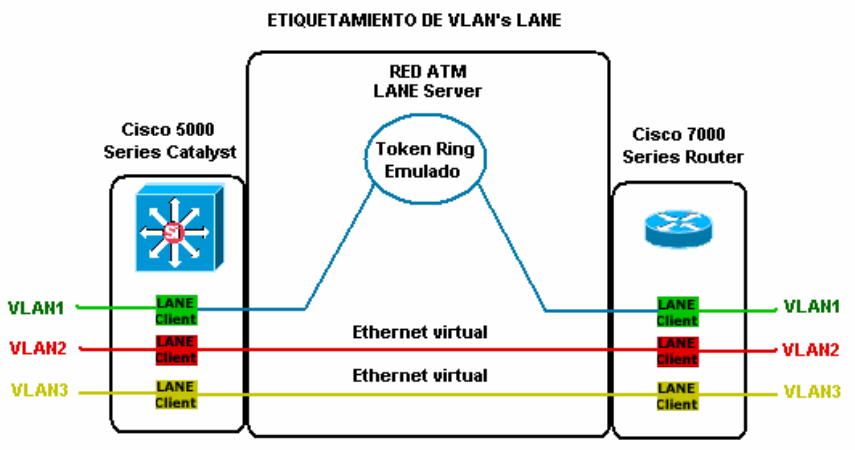


Figura 2.30 Etiquetado LANE

LANE emula los servicios lógicos de la capa 2 de Ethernet a través de dispositivos ATM. Con los servicios LANE, las VLANs puede automáticamente ser dispersadas a lo largo de múltiples LANs sobre una red ATM. Para lograr esto, un software especial de bajo nivel es implementado sobre las estaciones cliente ATM, llamado Cliente de Emulación LAN, o LEC, que trabaja con el Servidor de Emulación LAN, o LES para manejar todos los mensajes y paquetes que fluyen a través de la red, asegurando que los clientes no se enteren de la infraestructura de la red WAN, y así hacer que ésta sea

transparente. Por lo tanto LANE es una forma para hacer que una red ATM simule una red Ethernet. No hay etiquetamiento en LANE, pero la conexión virtual usada implica un VLAN ID.

2.3.4.3.2 IEEE 802.10

Es un protocolo usado en FDDI, que incorpora un mecanismo por medio del cual el tráfico LAN puede llevar un identificador VLAN. En la actualidad existen varios módulos disponibles para los switches Cisco, que permiten la integración de Ethernet en la red FDDI y con la ayuda del protocolo 802.10 se crea un mapeo entre la VLAN Ethernet y la red FDDI, permitiendo que todas las VLANs Ethernet estén disponibles para correr sobre la red FDDI.

2.3.4.3.3 Inter-Switch Link (ISL)

ISL es un protocolo propiedad de Cisco soportado solo por equipos Cisco, para etiquetar tramas Ethernet e identificar la información de las VLANs entre switches y routers, usado en enlaces FastEthernet y Gigabit Ethernet.

Este etiquetamiento de información permite a las VLANs ser multiplexadas sobre un enlace troncal a través de un método de encapsulación externo (ISL), el cual permite al switch identificar la membresía VLAN de la trama en el enlace troncal.

ISL, no altera la trama original, porque éste encapsula la trama Ethernet con una nueva cabecera de 26 bytes, que contiene al identificador VLAN (VLAN ID), y además añade un campo de secuencia de chequeo de trama (FCS ó CRC) de 4 bytes al final de la trama, como se muestra en la Figura 2.32. Por lo tanto, como la trama ha sido encapsulada por ISL con nueva información, solamente los dispositivos que conozcan ISL podrán leer estas nuevas tramas.

La información de VLAN ISL es añadida a la trama, solo si la trama es enviada por un puerto configurado como enlace troncal. Y la encapsulación ISL será borrada de la trama, si la trama es enviada por un enlace de acceso. Ver Figura 2.31.

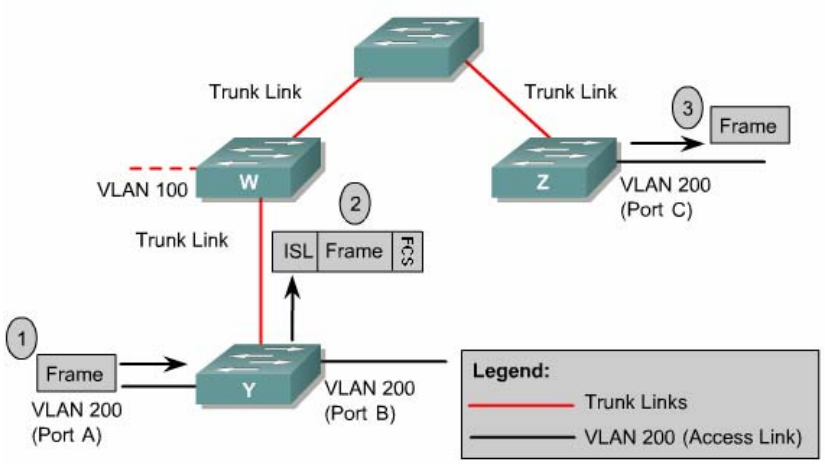


Figura 2.31 Protocolo de Encapsulación Inter-Switch Link[46]

ISL funciona en la capa 2 del modelo OSI, y es capaz de soportar hasta 1000 VLANs sin introducir ningún retardo en la transferencia de datos entre enlaces troncales.

ISL routing puede ser usado sobre el puerto de un swtich, la interfaz de un router y tarjetas de interfaz de red para troncalizar a un servidor. Esta es una muy buena aproximación si estamos creando VLANs funcionales y si no se quiere quebrantar la regla 80/20. Un **servidor troncalizado** es parte de todas las VLANs (dominios de broadcast) simultáneamente, es decir los usuarios no necesitan cruzar un dispositivos de capa 3 para acceder a éste. Esto es bueno porque reduce la latencia.

Estructura de la trama ISL

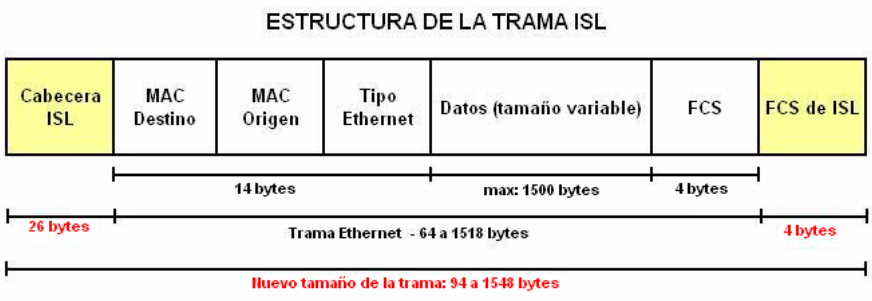


Figura 2.32 Estructura de la Trama ISL

El tamaño de la trama ISL puede ser desde 94 bytes e incrementarse hasta 1548 bytes. A continuación vamos a enfocarnos en los campos añadidos a la trama.

[46] Figura editada de Cisco CCNA3, Trunking Operation

- **Cabecera ISL**

  Este es un campo de 26 bytes conteniendo toda la información VLAN requerida, para permitir a la trama atravesar el enlace troncal y encontrar el camino a su destino.

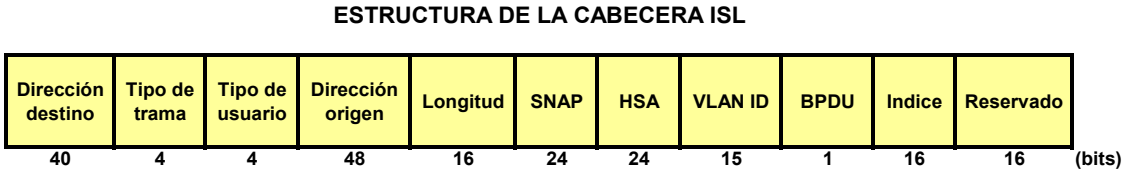


Figura 2.33 Estructura de la Cabecera ISL

- **Dirección de destino**

  Este campo es una dirección de destino de 40 bits que contiene una dirección de multicast, que usualmente es "0x01-00-0C-00-00" o "0x03-00-0C-00-00". Esta dirección es usada para indicar al receptor que la trama está en formato ISL.

- **Tipo de trama**

  Este campo de 4 bits de longitud ayuda a identificar la trama original encapsulada. Dependiendo del tipo de trama, éste campo puede tomar cuatro posibles valores como se muestra en la siguiente tabla:

Valor	Trama encapsulada
0000	Ethernet
0001	Token-Ring
0010	FDDI
0011	ATM

Tabla 2.1 Valores de los Tipos de Trama

- **Tipo de Usuario**

  El campo de usuario ocupando 4 bits sirve como una extensión del campo anterior "Tipo de trama", y es por lo común usado cuando la trama encapsulada original es una trama tipo Ethernet. Cuando esto sucede, los dos primeros bits del campo de usuario actúan como un mecanismo de priorización, permitiendo a las tramas encontrar el camino hacia el destino en una forma más fácil.

Valor	Prioridad de la trama
XX00	Prioridad normal
XX01	Prioridad 1
XX10	Prioridad 2
XX11	Prioridad alta

Tabla 2.2 Valores de las Prioridades de Trama

También debemos notar que el uso de prioridades es opcional y no es obligatorio.

- **Dirección de origen**

  Es la dirección MAC fuente del switch que está transmitiendo la trama. Este campo tiene 48 bits de longitud. El dispositivo de recepción puede elegir ignorar este campo.

- **Longitud**

  Este campo de 16 bits contiene la longitud total de toda la trama ISL menos los campos: dirección de destino, tipo de trama, tipo de usuario, dirección origen, longitud y FCS. Es decir la cantidad de información excluida es 18 bytes. Los campos de longitud en las tramas ayudan en la recepción final a identificar donde las porciones específicas de trama existen dentro de la trama recibida.

- **SNAP**

  El campo SNAP contiene 24 bits de longitud con un valor de: "0xAAAA03"

- **HSA**[47]

  Éste campo de 24 bits de longitud representa los 3 bytes superiores del campo "Dirección de origen" (porción ID de los fabricantes) y debe contener el valor "0x00-00-0C".

- **Identificador VLAN**

  Este quizás es el campo más importante de todos, porque éste permite a los enlaces troncales identificar a que VLAN pertenece la trama. El campo del VLAN ID es de

[47] High bits Source Address

15 bits de longitud y como se mencionó anteriormente éste es conocido como el "color" de la trama.

- **BPDU[48] e indicador CDP[49]**

  El campo BPDU solo tiene un bit de longitud pero es muy importante, tal como es configurado para todos los paquetes BPDU encapsulados por la trama ISL. Los BPDU's son usados por el protocolo *Spanning-Tree* para deshabilitar los enlaces redundantes y evitar los lazos de red. Este campo también es usado por tramas CDP y VTP que son encapsuladas. 0, no es enviado al CPU para procesamiento; 1, si es enviado al CPU para procesamient.

- **Índice**

  Este campo de 16 bits de longitud indica el índice del puerto del switch del cual sale el paquete. Este es solo usado para propósitos de diagnóstico y puede ser puesto cualquier valor por otros dispositivos.

- **Reservado para Token Ring y FDDI**

  Este campo es reservado cuando tramas Token Ring y FDDI son encapsulados en tramas ISL. En el caso de tramas Token Ring, los campos de Control de Acceso (AC) y Control de Trama (FC) son ubicados aquí, mientras que en el caso de FDDI, el campo FC es ubicado en el byte menos significativo (LSB) de este campo (si FC = "0x12" tendríamos un campo reservado = "0x0012"). Para tramas Ethernet el campo reservado es todo cero. Este campo tiene 16 bits de longitud.

- **FCS[50] de ISL**

  El campo de secuencia de chequeo de trama de ISL, de 4 bytes de longitud, asegura que la trama llegue intacta y que cualquier error sea detectado por el receptor. El FCS contiene un valor de 32 CRC, el cual es creado por la MAC de envio (switch) y éste es recalculado por la MAC receptora (switch) para chequear tramas corrompidas. El FCS de ISL es calculado en base a la trama entera ISL y añadida al final de ésta.

[48] Bridge Protocol Data Unit
[49] Cisco Discovery Protocol
[50] Frame Check Sequence

2.3.4.3.4 IEEE 802.1Q

El estándar IEEE 802.1Q especifica el etiquetamiento de tramas como un método para implementar VLANs. Insertando un campo de 4 bytes dentro de la trama Ethernet para identificar a que VLAN pertenece la información que se está transportando entre dispositivos de capa 2.

Características:

- Soporta hasta 4096 VLANs.
- Inserta un campo de 4 bytes sin encapsulación
- El tamaño de la trama final es más pequeña en comparación con ISL.

Restricciones:

Las troncales 802.1Q imponen algunas limitaciones en la estrategia trunking:

- "Los dispositivos que no son Cisco pueden soportar una instancia para todas las VLANs. Cuando se conecta un switch Cisco a un dispositivo no Cisco a través de una troncal 802.1Q, el switch Cisco combina la instancia s*panning-tree* de la VLAN de la troncal con la instancia s*panning-tree* del switch 802.1 Q no Cisco. Sin embargo, la información s*panning-tree* por cada VLAN es mantenida por switches Cisco separada por una nube de switches 802.1Q no Cisco.
- Asegurarse que la VLAN nativa para una troncal 802.1 Q es la misma en ambos extremos del enlace troncal, porque de lo contrario puede resultar en lazos s*panning-tree*.
- Si se deshabilita STP sobre la VLAN nativa de una troncal 802.1Q sin deshabilitar STP en cada VLAN de la red, potencialmente se pueden crear lazos STP. Es recomendable dejar habilitado STP en la VLAN nativa de una troncal 802.1Q o deshabilitar STP de todas las VLANs de la red. Asegurarse que la red esté libre de lazos antes de deshabilitar STP"[51].

[51] Creating and Maintaining VLANs, Chapter 8, Catalyst 3550.

Estructura de la trama IEEE 802.1Q

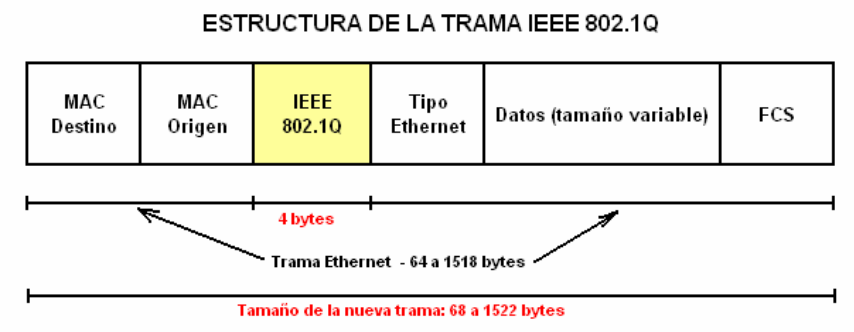


Figura 2.34 Estructura de la Trama IEEE 802.1Q

Debido a los 4 bytes extra, el tamaño mínimo de la trama Ethernet se incrementa de 64 a 68 bytes, mientras que el tamaño máximo de la trama Ethernet será **1522 bytes** de longitud. Estas nuevas longitudes máximas y mínimas de la trama CSMA/CD están contempladas en forma oficial por la **IEEE 802.3ac**.

Este método es el más popular por ser empleado por switches de diferentes fabricantes, ofreciendo compatibilidad de equipos. Incluso los switches Cisco pueden manejar este estándar.

El proceso de insertar el campo IEEE 802.1Q dentro de la trama Ethernet provoca que el campo FCS sea inválido, debido a que se alterado la trama, por lo tanto es esencial que un nuevo FCS sea recalculado, basado en la nueva trama que contiene al campo IEEE 802.1Q. Este proceso es automáticamente desarrollado por el switch antes de ser enviada la trama en el enlace troncal.

Cabecera IEEE 802.1Q

Esta cabecera es de 4 bytes o 32 bits de longitud, y dentro de ella está toda la información requerida para la identificación satisfactoria de las tramas a sus correspondientes VLANs y asegurar que estas arriben al destino correcto.

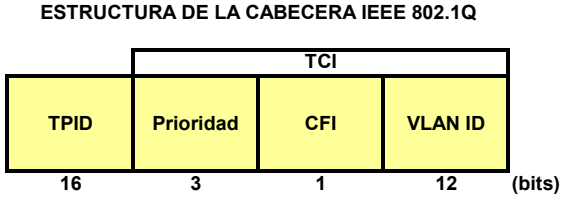


Figura 2.35 Estructura de la Cabecera IEEE 802.1Q

Esta estructura de 4 campos es sumamente más simple que la estructura ISL de 11 campos.

- **Identificador del protocolo de etiquetado (TPID)[52]**

  El TPID de 16 bits de longitud con un valor de 0x8100 es usado para identificar la trama como una trama etiquetada con IEEE 802.1Q / IEEE 802.1p.

  Los siguientes tres campos son conocidos como la **Información de control de etiquetado (TCI)[53]**, y a menudo es representado como un solo campo.

- **Prioridad**

  Este campo es usado para indicar la prioridad de los datos que está llevando la trama. La priorización de datos permite dar una especial prioridad al tiempo de latencia de servicios sensitivos, como la voz sobre IP (VoIP), sobre los datos normales. Esto significa que el ancho de banda especificado es asignado para estos servicios críticos y pasar a través del enlace sin ningún retardo. **(Campo de prioridad IEEE 802.1p)**

  Debido a que este campo consta de 3 bits, quiere decir que nos permite utilizar 8 (2^3=8) diferentes prioridades para cada trama, desde el 0 al 7.

- **Indicador de formato canónico (CFI)[54]**

  Este campo de 1 bit de longitud, si es asignado el valor de ´1´ quiere decir que la dirección MAC está en un formato no canónico, y si tiene el valor de ´0´ significa lo contrario. Para switches Ethernet este campo siempre es cero.

  Este campo es principalmente usado por razones de compatibilidad entre redes Token Ring y Ethernet. En el caso de que una trama arribe a un puerto Ethernet con la bandera CFI en 1, entonces la trama no será enviada a ningún puerto sin etiqueta (enlace de acceso) como este fue recibido.

[52] Tag Protocol Identifier
[53] Tag Control Information
[54] Canonical Format Indicador

- **Identificador VLAN**

  El campo VLAN ID al igual que en ISL, es posiblemente el campo más importante porque permite identificar a que VLAN pertenece la trama, permitiendo al switch receptor decidir porque puertos la trama puede salir dependiendo de la configuración del switch.

  La razón por la cual este protocolo de etiquetamiento (IEEE 802.1Q) puede manejar hasta 4096 VLANs, como se mencionó anteriormente, es porque el campo de VLAN ID está formado por 12 bits de longitud (2^12=4095), lo cual se traduce desde la VLAN 0 hasta la VLAN 4095.

  Un valor de VLAN ID de cero es usado para identificar tramas de prioridad y el valor 4095 es reservado, es decir el máximo número de VLANs configurables es 4094.

La Tabla 2.3 muestra un resumen de las características de los esquemas de etiquetamiento:

Métodos de encapsulación y etiquetado de trama			
Método de identificación	**Encapsulación**	**Etiquetado (dentro de la trama)**	**Medio**
802.1Q	No	Si	Ethernet
ISL	Si	No	Ethernet
802.10	No	No	FDDI
LANE	No	No	ATM

Tabla 2.3 Métodos de Encapsulación y Etiquetamiento de Trama

2.3.5 Enrutamiento entre VLANs

Las estaciones de trabajo dentro una VLAN viven en su propio dominio de broadcast y pueden comunicarse libremente. Las VLANs crean particiones de red y separación de tráfico en la capa 2 del modelo OSI, razón por la cual si queremos que dos estaciones de trabajo o cualquier otro dispositivo con direccionamiento IP se comuniquen entre VLANs, es absolutamente necesario un dispositivo de capa 3. La comunicación entre VLANs se puede conseguir por medio de conectividad física o lógica.

2.3.5.1 Conectividad Física

Ésta involucra una conexión física separada por cada VLAN, como se muestra en la Figura 2.36. Es decir que se necesita una interfaz física separada en el router por cada VLAN.

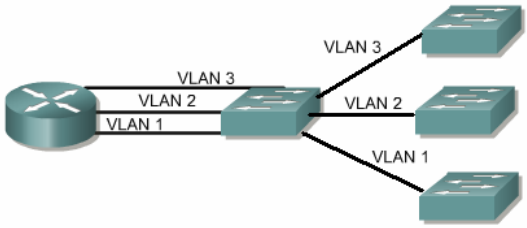


Figura 2.36 Conectividad Física

Si se pretende seguir con este tipo de conectividad, y si se tienen más VLANs que interfaces de router, una buena alternativa es utilizar un switch de capa 3 que reemplace al router, debido a que este tiene más puertos y puede funcionar como tal.

2.3.5.2 Conectividad Lógica

Es una simple conexión, o troncal, que transporta múltiples VLANs desde un switch a un router o switch de capa 3 (ver Figura 2.37), utilizando los métodos de encapsulamiento de *trunking*: Inter-Switch Link (ISL) o IEEE 802.1Q.

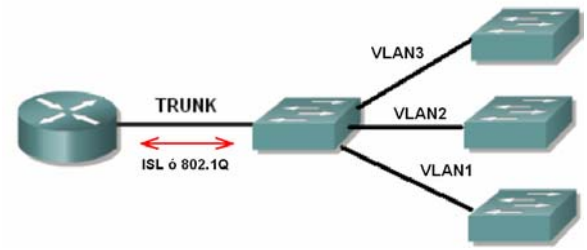


Figura 2.37 Conectividad Lógica con Trunking

Esta topología es conocida como: **"*router on a stick*"**

El tráfico entre VLANs debe cruzar el backbone de capa 2 para llegar al router donde éste puede moverse entre VLANs. Luego el tráfico viaja de vuelta a la estación final deseada, usando el normal reenvío de capa 2. Ver **¡Error! No se encuentra el origen de la referencia.**.

Generalmente hasta 255 VLANs puede manejar un router.

Cuando el número de VLANs se incrementa en una red, la idea de tener un router con diferentes interfaces por cada VLAN es in-escalable, razón por la cual, la forma más utilizada para manejar bastantes VLANs en la actualidad es usando *trunking* de VLANs con ISL o 802.1Q sobre enlaces Fast Ethernet (conectividad lógica). Ver Figura 2.38.

Además, para trabajar correctamente con enrutamiento entre VLANs, todos los routers y switches involucrados deben soportar y manejar el mismo tipo de encapsulamiento de *trunking*.

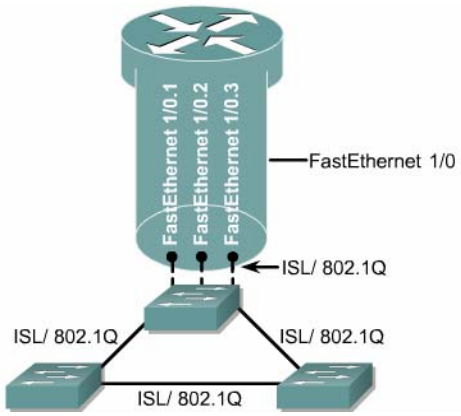


Figura 2.38 Router Conectado con Troncal[55]

Para permitir la comunicación entre VLANs por medio de un router con una sola conexión física (*router on stick*) hacia la LAN, es necesario la creación de sub-interfaces sobre la interfaz del router que se conecta a la red local.

2.3.5.3 División de Interfaces en Sub-interfaces

Una sub-interfaz es una interfaz lógica dentro de una interfaz física, tal como una interfaz Fast Ethernet en un router.

[55] Figura de Cisco CCNA3, Physical and logical interfaces

Varias interfaces lógicas o sub-interfaces pueden existir sobre una interfaz física. Por ejemplo la interfaz Fast Ethernet FastEthernet 0/0 puede soportar tres sub-interfaces numeradas así: FastEthernet 0/0.1, 0/0.2 y 0/0.3. Ver Figura 2.39.

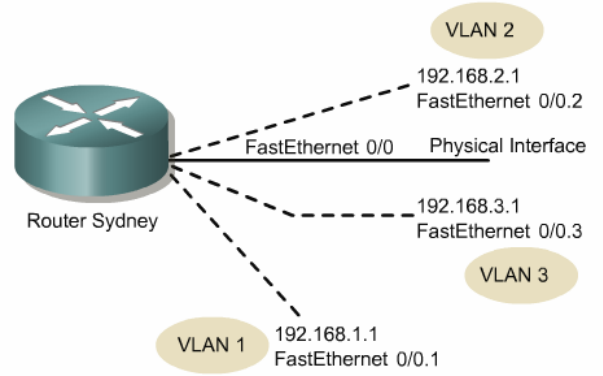


Figura 2.39 Subinterfaces y VLANs[56]

Cada sub-interfaz soporta una VLAN, y es asignada una dirección IP. Para que múltiples dispositivos en una misma VLAN se comuniquen, las direcciones IP de todas las sub-interfaces deben estar en la misma red o subred. Por ejemplo si la sub-interfaz FastEthernet 0/0.1 tiene una dirección IP de 192.168.1.1 entonces 192.168.1.2, 192.168.1.3 y 192.168.1.4 son direcciones de dispositivos conectados a la sub-interfaz FastEthernet 0/0.1.

Para enrutar entre VLANs con sub-interfaces, una sub-interfaz debe ser creada por cada VLAN.

2.3.6 VLAN Trunking Protocol -VTP

VTP fue creado por Cisco para resolver problemas operacionales en una red conmutada con VLANs.

Los dos problemas más comunes son:

- El cruce de VLANs causado por inconsistencias de configuración de VLANs.
- Falta de configuración de VLANs a través de medios mezclados como Ethernet y FDDI.

[56] Figura de Cisco CCNA3, Dividing physical interfaces into subinterfaces

Es decir el administrador de la red con la implementación de VTP evita configurar separadamente cada switch, una tarea que requiere una gran cantidad de tiempo y adiciona una gran cantidad de costos operativos dependiendo del tamaño de la red a parte que incrementa la posibilidad de errores o problemas de configuración.

El objetivo de VTP es mantener consistencia en la configuración de VLANs a través de un dominio de administración de red común. VTP es un protocolo de mensajes que usa las tramas de las troncales de capa 2 para añadir, eliminar y renombrar VLANs, información que luego es transmitida a todos los otros switches en el dominio del VTP. Un switch solo puede pertenecer a un solo dominio VTP.

2.3.6.1 Beneficios de VTP

- Consistente configuración de VLANs a través de todos los switches en la red.
- Permite a las VLANs ser troncalizadas sobre medios o redes mixtas, tales como de Ethernet a ATM LANE o incluso FDDI.
- Preciso rastreo y monitoreo de VLANs.
- Reporte dinámico de VLANs añadidas a todos los switches en el dominio VTP.
- *Plug-and-play* VLANs añadidas.

2.3.6.2 Operación de VTP

Un dominio VTP está constituido por dos o más dispositivos interconectados que comparten la misma información y nombre de dominio VTP.

Se puede usar un dominio VTP si se tiene más de un switch conectado en la red (lo contrario es irrelevante), pero si igual se tienen varios switches en una sola VLAN, no se necesita usar VTP. **La información VTP se envía entre switches solo vía enlaces troncales.**

Cuando se transmite mensajes VTP a otros swtiches en una red, los mensajes VTP son encapsulados en una trama de protocolo troncalizado tales como ISL o IEEE 802.1Q.

Las actualizaciones o base de datos de configuración VTP con adiciones o supresiones, son enviadas con un **número de revisión de configuración**, que es incrementado en uno. Cada vez que un switch recibe una actualización que tiene un número de revisión de configuración más alto, éste conoce que la información recibida es más actual, por lo tanto el switch sobrescribe la base de datos almacenada con la nueva información enviada en la actualización VTP. Además si una VLAN no existe en la nueva base de datos, ésta será borrada del switch. Ver Figura 2.40.

Cada aviso VTP comienza con un número de revisión igual a cero y se incrementará en 1 o n + 1 hasta que alcance el valor 2,147,483,648 cuando esto suceda el contador se resetea a cero. Además se dice que VTP mantiene su propia NVRAM porque aunque esta sea borrada, el número de revisión de la base de datos VTP no lo es. **Para que el número de revisión de configuración regrese a cero, el switch debe ser reseteado**.

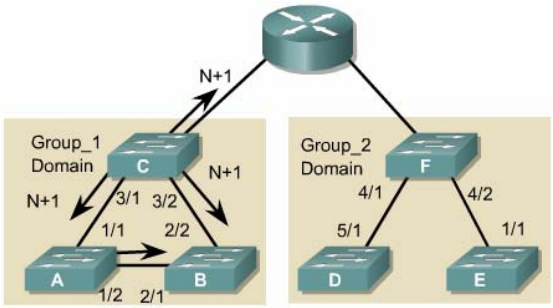


Figura 2.40 Operación VTP[57]

Con VTP, cada switch anuncia sobre sus puertos troncales: su dominio de administración, el número de revisión de configuración, las VLANs que conoce, y ciertos parámetros para cada VLAN conocida. Estas tramas son enviadas a una dirección multicast, es decir que todos los dispositivos vecinos pueden recibir las tramas. Sin embargo las tramas no son enviadas bajo procedimientos normales de bridging. Todos los dispositivos en el mismo dominio de administración aprenden acerca de cualquier nueva VLAN configurada en el dispositivo que está transmitiendo. Una nueva VLAN será creada y configurada sobre un solo dispositivo en el dominio de administración; todos los otros dispositivos en el mismo dominio de administración aprenden automáticamente la información.

[57] Figura de Cisco CCNA3, VTP Operation

Por defecto, los dominios de administración son establecidos en un modo no seguro, es decir los switches interactúan sin el uso de una clave o contraseña. Para que el dominio de administración cambie a modo seguro se añade una clave, y ésta deberá ser la misma en todos los switches pertenecientes al dominio.

Existen tres modos de operación para un switch dentro de un dominio VTP:

- Servidor
- Cliente
- Transparente

2.3.6.2.1 Servidor VTP

Al menos se necesita un servidor en un dominio VTP, para propagar la información de VLAN a lo largo del dominio. Los servidores VTP envían mensajes VTP por todos los puertos troncales. Ver Figura 2.41.

En este modo el switch puede crear, modificar o borrar VLANs y parámetros de configuración de las VLANs del dominio entero, y cualquier cambio realizado será notificado a todo el dominio VTP. El servidor VTP guarda la información de configuración de VLANs en la NVRAM del switch.

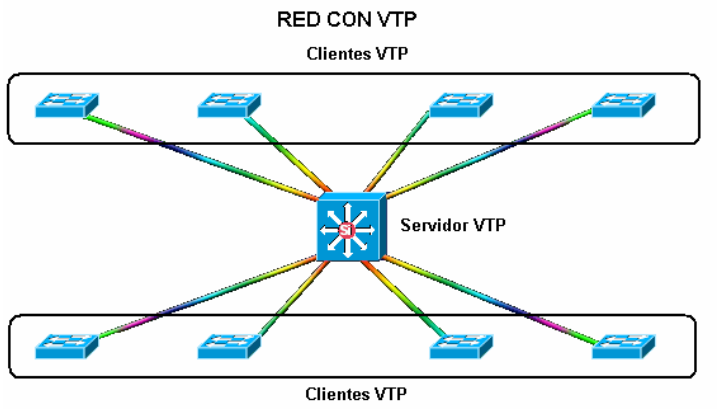


Figura 2.41 Red con VTP

2.3.6.2.2 Cliente VTP

En modo cliente, los switches reciben la información de los servidores VTP. El rol principal de un cliente VTP es procesar los cambios de las VLANs que se hayan recibido y

enviar mensajes VTP de actualizaciones por de todos los puertos troncales. Además no pueden crear, modificar o borrar información de VLANs.

Ninguno de los puertos de un switch cliente puede ser añadido a una nueva VLAN antes de que el servidor VTP notifique al switch cliente de la nueva VLAN. Este modo es útil para switches que no tienen suficiente memoria para almacenar grandes tablas de información VLAN.

Los switches clientes en cascada también reciben las actualizaciones VTP siempre y cuando estén enlazados con troncales y estén en el mismo dominio VTP, como se muestra en la Figura 2.42.

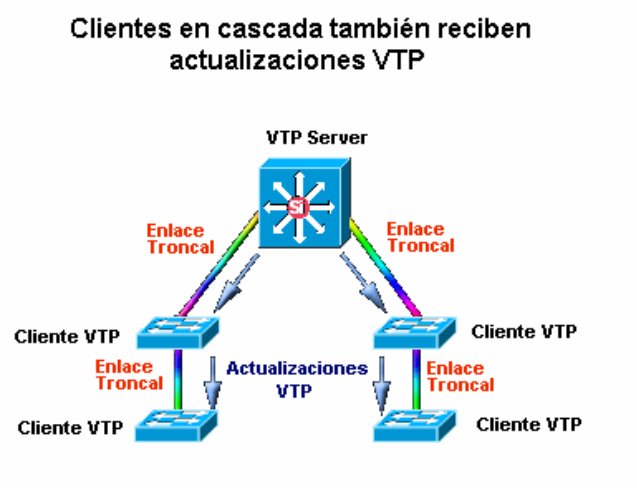


Figura 2.42 Clientes en Cascada reciben Actualizaciones VTP

Siempre es conveniente instalar a un nuevo switch como cliente VTP, y asegurarse que el número de registro de configuración es inferior al que tiene el servidor del dominio, porque si no es así, es posible que el nuevo switch envíe una nueva base de datos VTP a todos los otros switches, borrando así todas las VLANs existentes.

2.3.6.2.3 Transparente VTP

Los switches en modo transparente no participan en el dominio VTP, pero todavía envían avisos VTP a través de los enlaces troncales. Es decir un switch transparente no modifica su base de datos cuando recibe actualizaciones porque simplemente ignora el contenido de los mensajes.

Dependiendo de la versión del VTP, estos mensajes que son recibidos en el switch se envían fuera de sus puertos troncales a cualquier otro switch que puede estar conectado a este, si es la versión 2 de VTP (ver Figura 2.43); pero si es la versión 1 de VTP, entonces estos mensajes son simplemente ignorados y descartados por el switch.

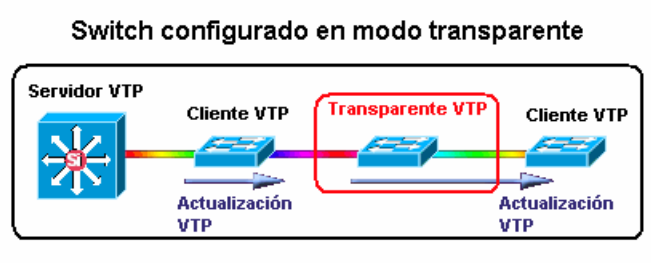


Figura 2.43 Switch en Modo Transparente con Versión 2 de VTP

Estos switches no pueden añadir ni borrar VLANs porque ellos mantienen su propia base de datos, la cual no es compartida con otros switches. Por lo tanto la base de datos de VLANs en modo transparente es realmente considerada local y aislada. Pero si pueden crear, modificar o eliminar VLANs en su switch local. Como es lógico, en este modo también se guarda la configuración de VLANs en la NVRAM del switch.

En la siguiente tabla se presenta un resumen de las características de los modos de operación VTP:

Característica:	Servidor	Cliente	Transparente
Enviar mensajes VTP	Si	Si	No
Recibir mensajes VTP	Si	Si	No
Crear VLAN's	Si	No	Si*
Recordar VLAN's	Si	No	Si*

* Localmente

Tabla 2.4 Características de los Modos de Operación VTP

Nota: Todos los mensajes VTP son enviados a través de la VLAN de administración que generalmente es la VLAN 1, que por regla no debe ser usado por nadie más que por los mismo switches. La creación de la VLAN de administración asegura que todos los switches tengan su propia red para comunicarse entre cada uno de ellos sin ninguna interrupción.

2.3.6.3 Estructura de los mensajes VTP

En la Figura 2.44 se muestra la encapsulación genérica para VTP dentro de una trama ISL.

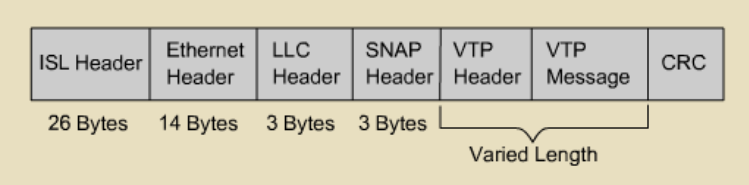


Figura 2.44 Trama de Encapsulación ISL con VTP[58]

La **cabecera VTP** varía en base al tipo de mensaje VTP, pero generalmente, los mismos cuatro ítems o campos son encontrados en todos los mensajes VTP:

- Versión del protocolo VTP: puede ser versión 1 o 2 (añade soporte para Token Ring).
- Tipo de mensaje VTP o código: indica uno de los cuatro tipos de mensaje.
- Longitud del nombre del dominio de administración: indica el tamaño de el nombre que sigue a continuación
- Nombre del dominio de administración: nombre configurado por el dominio de administración.

Existen dos tipos de avisos VTP:

- Peticiones de clientes que quieren información en el bootup
- Respuesta de servidores

Existen tres tipos de mensajes VTP:

- Aviso de resumen
- Aviso de subconjunto
- Petición de aviso

[58] Figura de Cisco CCNA3, VTP Operation

Con las peticiones de avisos, los clientes piden información de VLANs y los servidores responden con avisos resumen o subconjunto.

Existen también un cuarto mensaje que es utilizado en VTP *Pruning,* denominado: Mensaje de ingreso VTP.

2.3.6.3.1 Mensaje "Aviso de resumen"

Este es un mensaje publicado por todos los servidores de dominio VTP, Por defecto, los switches Cisco Catalyst servidores y clientes VTP, transmiten los Avisos Resumen cada cinco minutos.
Estos mensajes contienen la siguiente información adicional:

- **Número de revisión de configuración.-** identifica los nuevos cambios realizados en el dominio VTP. Se va incrementando en 1 cada vez que se hacen cambios en la configuración VTP.
- **Identidad actualizada**.- contiene la dirección IP del switch que incrementó por última vez el número de revisión de configuración.
- ***Timestamp* actualizado.-** entrega el tiempo de la última actualización que ha tenido lugar.
- **MD5[59] *Digest*.-** contiene la contraseña o clave VTP, en el caso que haya sido configurada y usada para asegurar la validación de la actualización VTP.
- **Seguidores.-** indica el número de mensajes "Avisos de subconjunto" que generalmente le siguen a mensajes "Aviso de resumen".

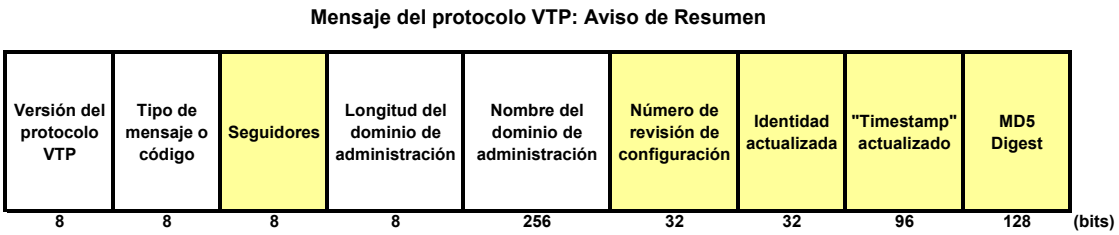


Figura 2.45 Mensaje del Protocolo VTP: Aviso de Resumen

[59] Message Digest 5

Cuando un switch recibe un mensaje "Aviso de resumen", éste primero compara el nombre del dominio de administración con el suyo propio. Si es diferente, entonces el mensaje es descartado y enviado fuera de sus enlaces troncales. Pero si son iguales los nombres de dominio, entonces chequea a continuación el número de revisión de configuración y si encuentra que es menor o igual que el suyo propio, entonces ignora el aviso; pero si encuentra que es mayor entonces el switch envía fuera un mensaje de "Petición de aviso" para nueva información VLAN.

2.3.6.3.2 Mensaje "Aviso de subconjunto"

Cuando se han realizado cambios en las VLANs, el servidor VTP envía publicaciones de "Aviso de resumen" seguido por el "Aviso de subconjunto". Dependiendo de cuantas VLANs estén configuradas en el dominio, existirán más de un "Aviso de subconjunto" para asegurar que la información de todas las VLANs está actualizada en todos los clientes VTP.

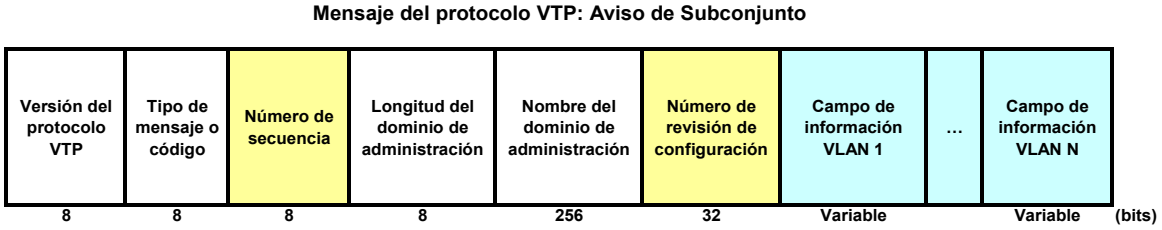


Figura 2.46 Mensaje del Protocolo VTP: Aviso de Subconjunto

En el campo código o tipo de mensaje para un "Aviso de subconjunto" va el valor "0x02".

Los dos nuevos campos en esta estructura son:

- **El número se secuencia.-** contiene la secuencia del paquete dentro de una cadena de paquetes siguiendo a un "Aviso de resumen". La secuencia comienza con 1 y se incrementa hasta el número de paquetes en la cadena.
- **Campo de información VLAN.-** Esta es la información VLAN que los switches están esperando.

El campo de información VLAN a su vez está descompuesto en los siguientes sub-campos:

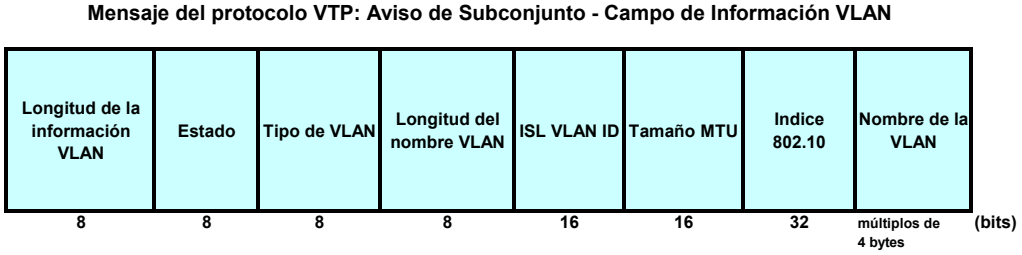


Figura 2.47 Aviso de Subconjunto – Campo de Información

Este campo de información VLAN contiene la información requerida solo para una VLAN, es decir si el dominio tiene varias VLANs y el "Aviso de subconjunto" ya ha sido enviado, el servidor VTP simplemente continuará enviando los "Campos de información VLAN" de las VLANs restantes.

Los sub-campos más importantes son la longitud del nombre VLAN, el identificador VLAN de ISL y el tamaño MTU, porque contienen información crítica acerca del anuncio de la VLAN en la trama particular de "Aviso de subconjunto". Además la presencia del campo que indica el tamaño del MTU confirma que cada VLAN es tratada como una red separada, donde incluso diferentes tamaños de MTU son posibles entre VLANs.

Existen ciertas acciones que provocan avisos de subconjunto, tales como:

- Creación o supresión de VLANs.
- Activación o suspensión de VLANs.
- Cambio de nombre de VLAN.
- Cambio en la unidad de transferencia máxima de VLAN.

2.3.6.3.3 Pedido de aviso

Cuando un switch cliente es apagado toda la información VTP almacenada en la RAM es perdida, y cuando lo encendemos toda su información debe reestablecerse, por lo tanto requiere ser actualizado con la última versión disponible en el servidor VTP.

Un switch cliente también enviará un "Pedido de aviso" cuando escuche un "Aviso de resumen" con un número de revisión más alto que el suyo.

Cuando un "Pedido de aviso" ha sido enviado al servidor VTP, éste responderá con un "Aviso de resumen", seguido de varios "Avisos de subconjunto" requeridos para informar a los clientes VTP acerca de la VLANs actualmente configuradas.

La siguiente figura muestra la estructura del mensaje "pedido de aviso":

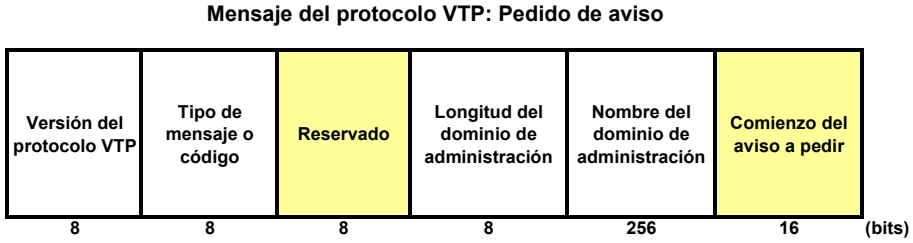


Figura 2.48 Mensaje del Protocolo VTP: Pedido de Aviso

Existen dos nuevos campos en esta estructura que son:

- **Reservado.-** generalmente no es usado por los "pedidos de aviso"
- **Comienzo del aviso a pedir.-** es el pedido actual enviado por el cliente VTP.

2.3.6.3.4 Mensaje de ingreso VTP

Este mensaje es enviado cuando un cliente VTP por primera vez ingresa a un dominio VTP, informando al servidor VTP acerca del nuevo cliente. Estos mensajes de ingreso VTP son similares a los mensajes de "pedido de aviso" pero con diferentes valores en el campo "tipo de mensaje" y unos pocos parámetros más.

2.3.6.4 VTP PRUNING

Los Broadcast y Unicast puede llegar a ser problema en redes con VLANs debido a que los switches se encuentran conectados con enlaces troncales, los cuales acarrean los broadcast a cada switch de la red, sin importar a que VLAN está proyectado éste broadcast

e incluso sin considerar si el switch final contiene puertos asignados a la VLAN interesada en el broadcast. Ver Figura 2.49.

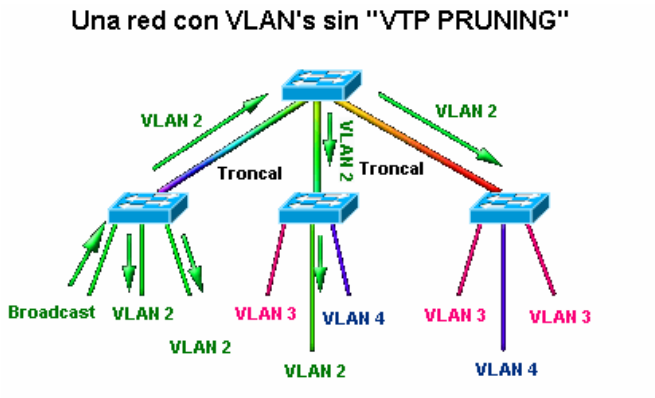


Figura 2.49 Red con VLANs sin VTP Pruning

Y éste problema realmente se agrava cuando tenemos una red grande con varios switches y caminos redundantes con enlaces troncales que interconectan estos equipos; fluyendo tráfico innecesario que consumen nuestro valioso ancho de banda.

Este problema se soluciona habilitando el VTP *Pruning* que reduce el flujo de tráfico innecesario es decir la cantidad de broadcast, multicast, y unicast de paquetes, preservando de esta forma nuestro ancho de banda. Y esto se consigue enviando broadcast y tramas unicast desconocidas de una VLAN sobre enlaces troncales solo si el dispositivo del otro extremo de la troncal tiene puertos en esta VLAN, como se muestra en la Figura 2.50.

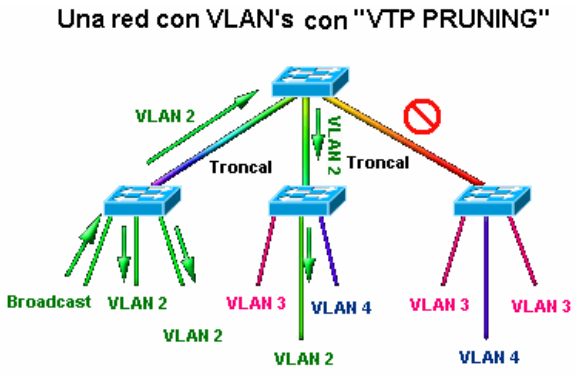


Figura 2.50 Red con VLANs con VTP Pruning

Cuando un switch tiene puertos asociados a VLANs, éste envía un anuncio a sus switches vecinos informándoles acerca de los puertos asignados a esas VLANs. Esta

información es almacenada por todos los vecinos y es usada para decidir si el tráfico de una VLAN debe ser enviada o no a ese switch vía puerto troncal.

Cuando se habilita VTP *Pruning* sobre el servidor VTP, se está habilitando para el dominio entero, excepto la VLAN 1 porque es la VLAN de administración, mientras que desde la VLAN 2 a la 1005 son elegibles.

VTP *Pruning* es soportado por ambas versiones de VTP. Con la versión 1 de VTP esto es con el uso de adicionales tipos de mensajes VTP.

Por defecto VTP *Pruning* está deshabilitado en todos los switches y puede ser habilitado en el o los servidores VTP de la red para que así se entere todo el dominio.

Una vez que se habilita VTP *Pruning* en la red, todas las VLANS son elegibles (con su excepción) para "*pruning*" en todos los enlaces troncales. Esta lista de elegibilidad de "*pruning*" puede ser modificada, configurando la lista "*Pruning-Eligible*" en cada uno de los puertos troncales deseados.

2.4 ESTÁNDARES Y PROTOCOLOS DE IEEE

El estándar **IEEE 802.1Q** es parte del estándar IEEE 802.1D. El estándar IEEE 802.1Q define una arquitectura para ***Virtual Bridged Local Area Networks,*** los servicios proporcionados en *Virtual Bridged LANs* y los protocolos y algoritmos en la provisión de esos servicios. En este estándar no hay mecanismos definidos para QoS[60], pero un importante requerimiento para proveer calidad de servicio está incluido en este estándar, que es la habilidad para regenerar la prioridad del usuario de las tramas recibidas usando la información de prioridad contenida en la trama y la Tabla de Regeneración de Prioridad del Usuario para el puerto de recepción.

La actualización del estándar **IEEE 802.1D** cubre todas las partes de las clases de tráfico acelerado y el filtrado multicast dinámico descrito en el estándar IEEE 802.1p.

[60] Quality of Service

2.4.1 IEEE 802.1p - Calidad de Servicio

El estándar **IEEE 802.1p** también es una parte del estándar IEEE 802.1D. El estándar IEEE 802.1p trata sobre la clase de tráfico acelerado (o priorización de tráfico) y el filtrado de multicast dinámico, además de describir importantes métodos para proveer calidad de servicio (QoS) a nivel de MACs.

La especificación de priorización de tráfico trabaja en la capa 2 del modelo OSI; y el filtrado de tráfico multicast es para asegurar que éste no proliferará sobre las redes conmutadas de capa 2.

Este protocolo también puede ser definido como *best-effort* QoS o CoS[61] en la capa 2 y es implementado en adaptadores de red y switches sin involucrar ninguna restricción. El tráfico 802.1p es simplemente clasificado y enviado al destino, sin reservaciones de ancho de banda establecidas.

IEEE 802.1p es una extensión del estándar IEEE 802.1Q, es decir ellos trabajan en *tandem*. Uno de los campos en la estructura 802.1Q es el de Priorización (3 bits), pero realmente este no trabaja con éste estándar, con el cual está definido es con el estándar 802.1p, campo que permite a los paquetes ser agrupados en varias clases de tráfico.

IEEE 802.1p establece ocho (2^3=8) niveles de prioridad. IEEE hace algunas recomendaciones. La prioridad más alta es siete, el cual es para tráfico de red crítico tal como tablas de actualización de *Routing Information Protocol (RIP)* y *Open Shortest Path First (OSPF)*. Los valores cinco y seis podrían ser para aplicaciones sensitivas al retardo tales como video interactivo y voz. Las clases de datos para el rango del cuatro al uno son aplicaciones de carga controlada tales como "*stream multimedia",* y tráfico crítico de negocios llevando datos SAP, por ejemplo al dar de baja tráfico "*loss eligible*". El valor cero es usado como un mejor esfuerzo por defecto, invocado automáticamente cuando ningún otro valor ha sido configurado.

Ver detalles de la estructura de la trama IEEE 802.1Q en la Figura 2.35 Estructura de la Cabecera IEEE 802.1Q.

[61] Class of Service

Aunque la mayoría de los fabricantes están de acuerdo que el estándar 802.1p es el mecanismo para etiquetar tramas para priorización, no existe un solo acercamiento uniforme para implementar el uso de los valores que puede tomar el campo de priorización. Muchos fabricantes soportan solo dos o tres valores de prioridad en sus switches de los ocho que existen. Por ejemplo un switch puede tomar los valores del 0 al 3 como prioridad baja, y los valores desde el 4 al 7 son con máxima prioridad.

De acuerdo al estándar IEEE 802.1p los siguientes parámetros son esenciales para proveer calidad de servicio (QoS):

1) Disponibilidad de servicio.
2) Pérdida de trama.
3) Falla en el orden de la trama.
4) Duplicación de trama.
5) El retardo de tránsito experimentado por las tramas.
6) Tiempo de vida de la trama.
7) La no detección de la taza de error de la trama
8) Máximo tamaño soportado por la unidad de datos de servicio.
9) Prioridad del usuario.
10) *Throughput.*

1) Disponibilidad de servicio

La disponibilidad de servicio es medida como la relación entre la disponibilidad y no disponibilidad del servicio MAC. Con el propósito de incrementar la reconfiguración automática de la disponibilidad de servicio de la *Bridged Local Area Network*, esta debe ser adoptada.

2) Pérdida de trama

El servicio MAC no provee una entrega garantizada de las Unidades de Datos de Servicio, pero la probabilidad es alta. Las pérdidas de trama pueden ocurrir debido a:

a) Corrupción de la trama en la capa física
b) La trama es descartada por el bridge debido a:
    a. La trama ha alcanzado el máximo tiempo de vida.

b. Agotamiento de la capacidad de buffering interno.
c. El tamaño de la trama Unidad de Datos de Servicio es muy grande para la LAN.
d. *Bridged Local Area Network* es forzada a descartar tramas para mantener otros aspectos del QoS.

3) Falla en el orden de la trama

El servicio MAC no permite el reordenamiento de tramas con la misma prioridad de usuario para un par de direcciones de destino y origen.

4) Duplicación de trama

El servicio MAC no permite la duplicación de tramas.

5) Retardo de tránsito

El retardo de tránsito de la trama es el tiempo transcurrido entre un pedido MA_UNITDATA y su correspondiente indicación MA_UNITDATA sobre una transferencia satisfactoria.

6) Tiempo de vida de la trama

Si el máximo retardo de una trama que ha sido impuesto por todos los bridges en el *Bridged Local Area Network* , excede el tiempo de vida máximo deseado, la trama debe ser descartada.

7) No detección de la taza de error de la trama

Usando los cálculos de FCS para cada trama, la no detección de la taza de error de la trama es muy baja.

8) Máximo tamaño soportado por la unidad de datos de servicio.

Este parámetro depende del medio de acceso usado. Un bridge entre dos LANs tiene un tamaño de unidad de datos de servicio, del que sea más pequeño.

9) Prioridad

El servicio MAC cuenta la prioridad de usuario como un parámetro del QoS

10) *Throughput*

El total *Throughput* de una *Bridged Local Area Network* puede ser tan grande como una de sus LANs equivalentes.

2.4.1.1 Definición de Calidad de Servicio (QoS)

No es fácil encontrar una definición para la calidad de servicio. Cada servicio tiene su propia definición para QoS y cada servicio puede ser descrito por sus características QoS. Para el desempeño de una red de comunicación de datos, las características QoS son: ancho de banda, retardo y confiabilidad. Estas características para su desempeño incluyen:

- **Ancho de Banda**: Taza de datos pico (PDR), Taza de datos continua (SDR), Taza de datos mínima (MDR).
- **Retardo**: *End-to-end* o *Round-Trip Delay*, Variación de retardo (*Jitter*).
- **Confiabilidad**: Disponibilidad (como % *uptime*), promedio de tiempo entre fallas / promedio de tiempo para reparar (MTBF/MTTR), errores y pérdidas de paquetes.

Por lo tanto para determina el QoS de una red, es necesario conocer las aplicaciones y servicios utilizados en la red.

2.5 PROBLEMAS EN TOPOLOGÍAS REDUNDANTES

En la actualidad muchas compañías y organizaciones confían o dependen de las redes de computadoras para sus operaciones. El acceso a servidores de archivos, bases de datos, internet, intranets y extranets es crítico para el éxito de los negocios. Y si por alguna razón éstas redes caen, tanto la productividad de la empresa como el servicio al cliente también caen.

Estas son algunas de las importantes razones por las cuales se debe tener redes confiables, que se consigue a través de equipos que también sean confiables y diseños de red que toleren fallas o anomalías. Diseños de red que deben converger rápidamente para pasar por alto estas fallas.

Y esta confiabilidad en las redes se incrementa a través de la redundancia de caminos y equipos en la red. Topologías redundantes que eliminan puntos únicos de falla. Si un enlace o dispositivo falla, simplemente el enlace o dispositivo redundante o de backup, toma las funciones o envío de tráfico del camino o equipo que ha fallado. Ver Figura 2.51.

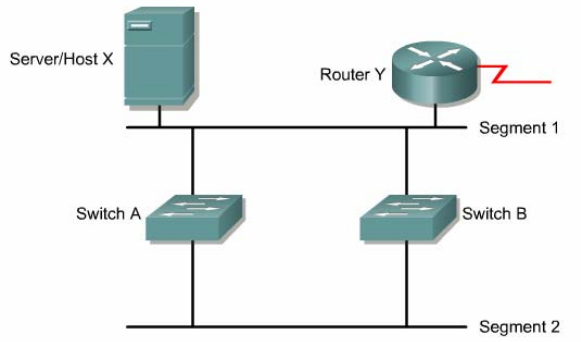


Figura 2.51 Topología Redundante Simple[62]

Pero lamentablemente una topología conmutada redundante causa otros problemas, como:

- Tormentas de broadcast
- Múltiples copias de tramas
- Inestabilidad en la tabla de direcciones MAC

2.5.1 Tormentas Broadcast

Las tramas broadcast y multicast son inundadas en todos los puertos excepto en el cual fue recibida la trama. Los multicast son tratados como broadcast por los switches.

"Por ejemplo, como en la Figura 2.52, si el host X envía un broadcast, como un pedido ARP para la dirección de capa 2 del router, entonces tanto el switch A como el switch B, también envían broadcast hacia fuera de todo sus puertos, y así los switches continúan propagando el tráfico de broadcast una y otra vez. Esto se denomina tormenta de broadcast, y continuará hasta que uno de los switches sea desconectado. Lo que produce que se reduzca el tráfico del usuario, y que la red caiga o sea extremadamente lenta"[63].

[62] Figura de Cisco CCNA3, Redundant switched topologies
[63] Ejemplo tomado de Cisco CCNA3, Broadcast Storm

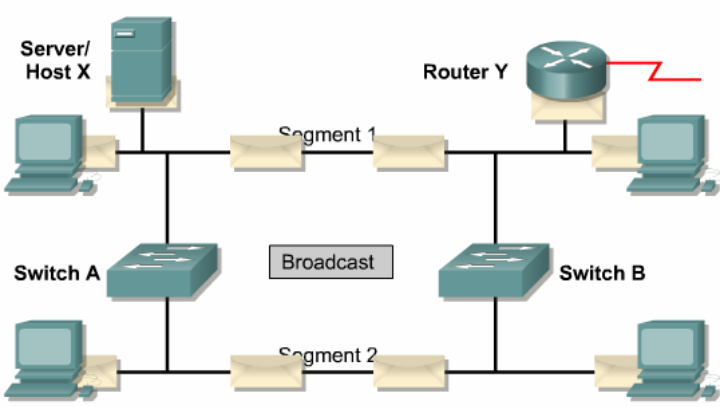


Figura 2.52 Tomentas Broadcast[64]

2.5.2 Transmisión de Tramas Múltiples

En topologías redundantes, es posible que un dispositivo final reciba múltiples tramas. "Por ejemplo si un host X envía una trama unicast a un router, como en la Figura 2.53, y si asumimos que los switches no conocen la dirección MAC del router, entonces por el proceso que se conoce como "***flooding***", estos switches también enviaran la misma trama al router"[65]. Lo cual resulta en una utilización innecesaria de los recursos de red.

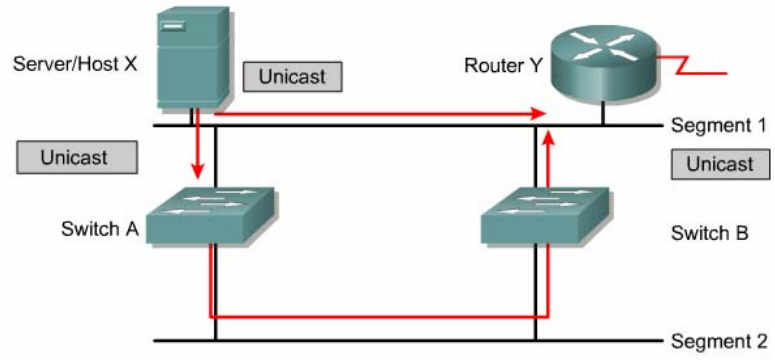


Figura 2.53 Transmisión de Tramas Múltiples[66]

2.5.3 Inestabilidad en la tabla de Direcciones MAC

En una red conmutada redundante es posible que los switches aprendan información incorrecta.

[64] Figura de Cisco CCNA3, Broadcast Storm
[65] Ejemplo tomado de Cisco CCNA3, Multiple frame transmissions
[66] Figura de Cisco CCNA3, Multiple frame transmissions

"Un switch puede aprender incorrectamente que una dirección MAC es en un puerto, cuando actualmente está en otro puerto diferente"[67].

"Por ejemplo si el host X envía una trama dirigida al router Y, tanto el switch A como el B aprenden que el host X está en el puerto 0, luego como tampoco estos switches tienen en sus tablas la dirección del router, (al igual que en el anterior caso por "*flooding*") envían la trama al router Y por el puerto 1, como ambos switches reciben la información por el puerto 1 entonces incorrectamente aprenden que la dirección MAC del host X está en el puerto1. Y cuando el router Y envíe una trama al host X, los switches A y B lo enviarán hacia fuera del puerto 1, lo cual es incorrecto"[68] Ver Figura 2.54.

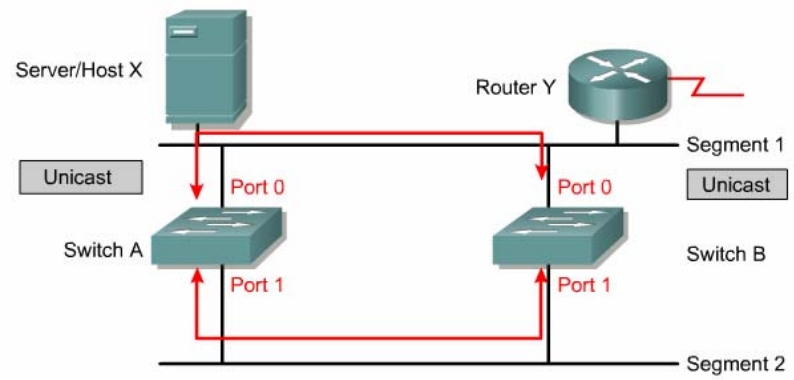


Figura 2.54 Inestabilidad en la Base de Datos MAC[69]

Este ejemplo de la trama unicast del router Y al host X, será capturada en un lazo.

2.6 PROTOCOLO SPANNING-TREE (STP)

Una red conmutada introduce enlaces redundantes entre los swicthes y bridges para sobreponerse a las fallas de un solo enlace, es decir para dar confiabilidad a la red. Pero estas conexiones introducen lazos físicos dentro de la red que a su vez generan lazos de tráfico. Es necesario señalar además, que tanto el tráfico generado por el proceso "flodding" de un switch, como los broadcast y multicast, pueden ser capturados en lazos, que provocan: la reducción del tráfico del usuario debido al congestionamiento, la utilización innecesaria de los recursos de red o el envío de tramas a destinos equivocados.

[67] Cisco CCNA3, Media access control database instability
[68] Ejemplo tomado de Cisco CCNA3, Media access control database instability
[69] Figura de Cisco CCNA3, Media access control database instability

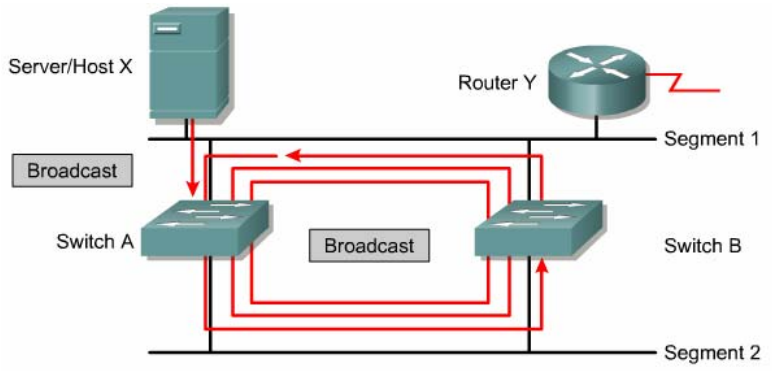


Figura 2.55 Red con Tormentas Broadcast sin STP[70]

La solución para tener una red confiable, con lazos físicos pero sin lazos de tráfico, es utilizar una topología lógica libre de lazos. Esta topología es el *Spanning-Tree*, que es una topología lógica en estrella o estrella extendida (como un árbol) de la red, en donde todos los dispositivos son alcanzables.

Es decir el protocolo *Spanning-Tree* (STP) evita lazos de tráfico que han sido formados cuando switches o bridges están interconectados vía múltiples caminos. El protocolo *Spanning-Tree* está basado en el algoritmo IEEE 802.1D intercambiando mensajes BPDU's (*Bridge Protocol Data Unit*) con otros switches para detectar lazos, y luego eliminar estos lazos deshabilitando o bloqueando las interfaces de los switches que llevan a enlaces redundantes que no son parte del árbol de rutas más cortas, garantizando que solamente hay uno y solamente un camino activo entre dos dispositivos de red.

Por lo tanto este protocolo realiza básicamente dos funciones:

- Elimina lazos en una red con enlaces redundantes seleccionando el bloqueo o deshabilitación de ciertos enlaces.
- Monitorea la red, para en caso de falla de enlaces activos, reactivar los enlaces redundantes y reestablecer la red, (disminuyendo así el "*downtime*"), manteniendo la topología lógica libre de lazos.

El protocolo *Spanning-Tree* establece un nodo raíz llamado *root bridge*. Luego construye una topología que tiene un camino por cada nodo en la red, con la ayuda de los

[70] Figura de Cisco CCNA3, Redundant topology and Spanning-Tree

mensajes BPDU's. Este árbol se origina desde el *root bridge*, y los enlaces redundantes que no son parte del árbol de caminos más cortos son bloqueados.

2.6.1 Operación de los Switches con Spanning-Tree

Las acciones que realizan los switches, gracias a la información que les llega con el mensaje BPDU, son las siguientes:

- Selecciona a un solo switch como el nodo raíz, conocido como "*Root Bridge*", de donde se va a originar todo el árbol de rutas.
- Calcula la ruta más corta desde si mismo hasta el nodo raíz. El camino más corto ésta basado en el costo del enlace acumulativo, y este costo a su vez se basa en la velocidad del enlace. Ver Tabla 2.5.

Velocidad de enlace	Costo (Revisado por IEEE)	Costo (Previo a IEEE)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

Tabla 2.5 Costos de los Enlaces Spanning-Tree

- Designa a uno de los switches como el más cercano al switch raíz. Este switch es llamado "Switch Designado", quien se encarga de todas las comunicaciones desde el segmento LAN hasta el "*Root Bridge*".
- Selecciona a uno de sus puertos como su "Puerto Raíz", para cada switch que no es nodo raíz. Esta interfaz entrega el mejor camino hacia el nodo raíz.
- Elige puertos que son parte del *Spanning-Tree*. Estos puertos se los denomina "Puertos Designados", y existe uno solo por cada segmento. Los "Puertos no Designados" son **bloqueados** es decir descartan el tráfico de datos pero si aceptan los BPDU's, lo cual asegura que si un camino activo o dispositivo falla, un nuevo *Spanning-Tree* puede ser calculado.

2.6.2 Elementos de una red Spanning-Tree

En una red con *Spanning-Tree* los elementos que existen son:

- Un *root bridge* por red
- Un puerto raíz (F) por cada switch que no es *root bridge.*
- Un puerto designado (F) por segmento
- Puertos no designados (B)

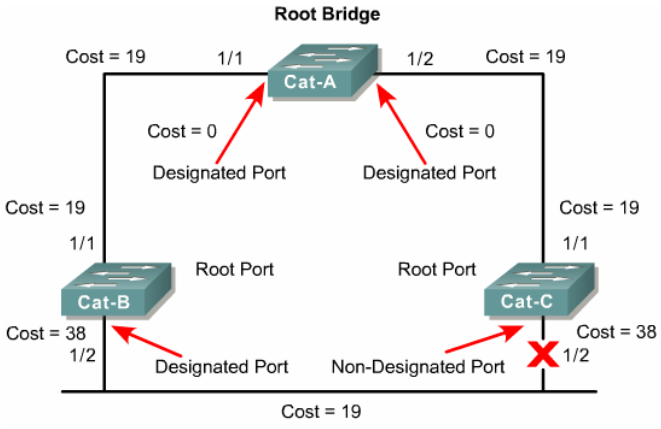


Figura 2.56 Elementos de una Red Spanning-Tree[71]

2.6.3 Estructura de un BPDU

Por defecto los BPDU's son enviados cada dos segundos. El mensaje BPDU está formado por los siguientes campos:

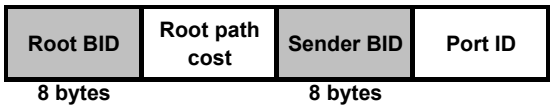


Figura 2.57 Estructura de un BPDU

- ***Root BID.-*** indica que switch es el *root bridge*
- ***Root path cost.-*** indica el costo del camino hacia el nodo raíz, o que tan lejos estamos de él.
- ***Sender BID.-*** Indica el BID del switch que envía este BPDU.
- ***Port ID.-*** Indica el puerto del switch del cual proviene el BPDU.

[71] Figura de Cisco CCNA3, Spanning-tree protocol

El identificador de switch/bridge o BID consiste de un campo llamado *bridge priority* o *switch priority* que por defecto es 32768 y de la dirección MAC del switch. Ver Figura 2.58.

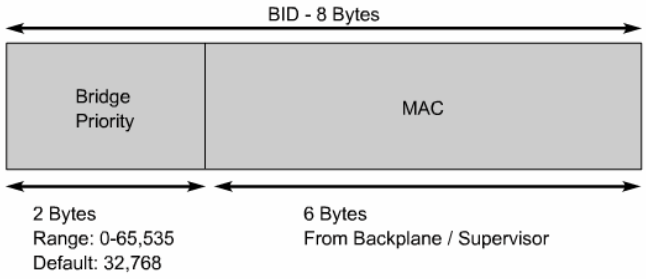


Figura 2.58 Identificador de Switch / Bridge (BID)[72]

Lo primero que realiza el protocolo *Spanning-Tree* en un switch cuando es iniciado, es determinar el *root bridge.*

2.6.4 Identificador de Sistema Extendido

Debido a que cada VLAN es considerada como un *logical bridge* diferente con PVST[73]+ y *rapid* PVST+, el mismo switch debe tener varios *bridge IDs* como VLANs configuradas sobre este.

Cada VLAN en el switch tiene un único *bridge ID que* está formado por 16 bits ó 2 bytes para el *bridge priority* y 6 bytes para la dirección MAC del switch, lo cual es sin habilitar el identificador de sistema extendido o *Extended System ID.* Ver Tabla 2.6.

Bridge Priority Value															
Bit 16	**Bit 15**	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Tabla 2.6 Bridge Priority con el Extended System ID deshabilitado[74]

En switches como los Catalyst 3550 ó 4500, desde las actualizaciones de IOS de Cisco: 12.1(18)EA1 y 12.1(12c)EW, respectivamente, éstos soportan las extensiones *Spanning-Tree* 802.1T; es decir estos switches pueden habilitar el *extended system ID,* lo

[72] Figura de Cisco CCNA3, Selecting the root bridge
[73] Per VLAN Spanning-Tree
[74] Tabla del Catalyst 4500 Series Switch Cisco IOS Configuration Guide, Chap-Pág. 15-4

cual implica que el *bridge priority* ahora es un valor de 4 bits y a su vez el *extendend system ID* es un valor de 12 bits. Ver tabla zz

Bridge Priority Value				**Extended System ID (Set Equal to the VLAN ID)**											
Bit 16	**Bit 15**	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**
32768	16384	8192	4096	VLAN ID											

Tabla 2.7 Bridge Priority con el Extended System ID habilitado[75]

Nota: *Spanning-Tree* usa el VLAN ID como *Extended System ID*.

Por lo tanto STP usa el *extended system ID*, el *switch priority* y la dirección MAC STP adjudicada para construir el único *bridge ID* por cada VLAN. En las anteriores versiones, cuando los switches no usan esta característica del *extended system ID*, STP usa una dirección MAC por VLAN para construir un único *bridge ID* por cada VLAN.

2.6.5 Selección del Root Bridge

Cuando un switch se está inicializando éste asume que éste es el *root bridge* y envía BPDU's que contienen la dirección MAC del switch tanto en el *root BID* como en el *sender BID*. Luego los BID's son recibidos por todos los switches y éstos reemplazan los *root BID's* más altos con *root BID's* más bajos en los BPDU's que son enviados fuera. Todos los switches reciben los BPDU's y determinan que el switch con el menor valor *root BID* será el *root bridge.*

Los administradores de red pueden configurar la prioridad de los switches a un valor más pequeño que el que está por defecto, lo cual hace más pequeño el BID. Esto debe ser implementado cuando el flujo de tráfico de la red es bien entendido. Además considerar que la posición del *root bridge* en la red, afecta el tráfico de la red.

2.6.6 Estados de los Puertos Spanning-Tree

Existen cuatro estados en los puertos de un switch que usa *Spanning-Tree*, estos son:

[75] Tabla del Catalyst 4500 Series Switch Cisco IOS Configuration Guide, Chap-Pág. 15-4

- **Estado de Bloqueo**.- recibe solo los mensajes BPDU. Descarta las tramas de datos y no hay direcciones que pueda aprender. Este estado puede durar unos 20 seg.
- **Estado de Escucha**.- construye una topología activa. Descubre si existen otros caminos hacia el *root bridge*, y si estos caminos no tienen el menor costo serán bloqueados. Este periodo de escucha es conocido como "*forward delay"* y dura 15 segundos.
- **Estado de Aprendizaje**.- construye una tabla de bridging. En este estado los datos no son enviados, pero las direcciones MAC son aprendidas desde el tráfico recibido. Este estado dura 15 segundos y también es llamado "*forward delay"*.
- **Estado de Envío**.- envía y recibe datos. Las direcciones MAC continúan siendo aprendidas y los BPDU's todavía son procesados.

Los puertos pueden estar en un **estado deshabilitado**, que puede ocurrir cuando un administrador *shut down* el puerto o el puerto está fallando.

Los tiempos dados a cada estado son por defecto, y fueron calculados asumiendo un máximo de siete switches por rama del *Spanning-Tree* desde el *root bridge.*

Cuando una topología de red cambia, los switches y bridges recalculan el *Spanning-Tree* y esto causa una discontinuidad en el tráfico de la red. La convergencia de una nueva topología *Spanning-Tree* que usa el estándar IEEE 802.1D puede tomar hasta 50 segundos, que resulta de la suma de los tiempos los estados de bloqueo, escucha y aprendizaje.

2.6.7 Variaciones del Protocolo Spanning-Tree

2.6.7.1 Common Spanning-Tree (CST / 802.1D)

Asume una instancia s*panning-tree* para toda la red *bridged*, sin considerar el número de VLANs. Esta implementación reduce la carga CPU desde que solamente una instancia s*panning-tree* es mantenida para la red entera. Esta implementación es típicamente usada cuando solamente una topología de capa 2 es necesaria en la red.

2.6.7.2 Multiple Instance STP (MISTP / 802.1s)

Es un estándar de la IEEE que permite algunas VLANs ser mapeadas para reducir el número de instancias s*panning-tree*. Esto es posible desde que la mayoría de redes no necesitan más que una pocas topologías lógicas. Cada instancia maneja múltiples VLANs que tienen la misma topología de capa 2.

2.6.7.3 Per-VLAN Spanning-Tree (PVST)

Mantiene una instancia s*panning-tree* por cada VLAN configurada en la red. Está es usada por el protocolo de *trunking* ISL y permite a una trocal VLAN enviar algunas VLANs mientras otras están bloqueadas. Desde que PVST trata a cada VLAN como una red separada, este puede hacer carga balanceada de tráfico (en capa 2), enviando algunas VLANs sobre una troncal y otras VLANs sobre otra troncal sin causar un lazo s*panning-tree*.

2.6.7.4 Rapid Spanning-Tree (RSTP / 802.1w)

Es una evolución del protocolo *Spanning-Tree* (estándar 802.1D) que provee una convergencia más rápida del s*panning-tree* después de un cambio de topología. Este estándar también incluye características equivalentes a Cisco PortFast, UplinkFast y BackboneFast para una reconvergencia de la red más rápida.

Este estándar introduce nuevas características como:

- Clarifica los roles y estados de los puertos
- Se definen unos de tipos de enlaces que pueden ir rápidamente al estado de "Envío".
- Se permite que los switches en una red con convergencia generen BPDU's en lugar de utilizar BPDU's del *Root Bridge*

El estado de bloqueado de un puerto es renombrado como estado de "Descartado". El rol de este puerto es el de un puerto alterno. El puerto descartado llega a ser un puerto designado, si este último falla en el segmento.

Existen 3 tipos de enlaces definidos como *point-to-ponit*, *edge-type* y *shared*. Estos cambios permiten que los enlaces con fallas sean descubiertos de forma más rápida. Los enlaces *point-to-point* y *edge-type* puedan ir al estado de "Envío" inmediatamente. La convergencia de la red no demorará más de 15 segundos, con estos cambios.

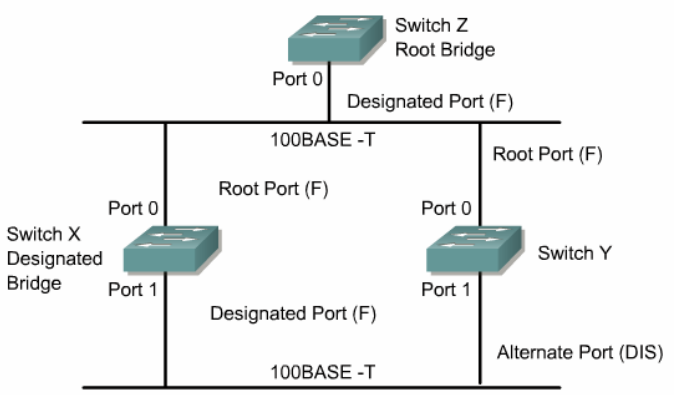


Figura 2.59 Designación de Puertos RSTP[76]

2.6.7.5 Per-VLAN Spanning-Tree Plus (PVST+)

Provee la misma funcionalidad que PVST usando la tecnología de *trunking* 802.1Q en lugar de ISL. PVST+ es una mejora propietaria del estándar 802.1Q y no es soportada sobre dispositivos no Cisco.

[76] Figura de Cisco CCNA3, Rapid Spanning-Tree protocol

CAPITULO III

REDISEÑO DE LA RED

3.1 REDISEÑO DE LA RED LA MATRIZ DE PETROCOMERCIAL

Aprovechando la compra de los nuevos equipos de red y el remodelamiento de los edificios El Rocio y Ex-Salesianos, especialmente en lo referido a cableado estructurado y la reubicación del cuarto principal de comunicaciones, se propone un rediseño completo de esta red.

3.1.1 Análisis de la Red Actual de la Matriz

Previo al diseño de la nueva red, vale hacer hincapié en los problemas de la red actual. La red de los edificios El Rocio y Ex-Salesianos, básicamente tiene una topología tipo bus con un backbone físico formado por fibra óptica, lamentablemente con dos grabes cuellos de botella previos a los servidores y sistemas I-Series (AS/400) por utilizar medios que máximo soportan 100Mbps (Figura 3.1), cuando obviamente estas rutas son las más congestionadas y la empresa está en la capacidad de ofrecer un medio con mejor ancho de banda. Además de tener conectado estos equipos a un switch de capa 2, cuando al menos deberían estar conectados a un switch multilayer o a un switch de core para proveer un mejor desempeño del tráfico, debido a que estos dispositivos manejan mejores velocidades de procesamiento. Igualmente los equipos que proveen los diferentes accesos (routers), no están conectados directamente al backbone, lo cual es aconsejable en lugar de tenerlos en la capa de acceso, para conseguir que el tráfico de la WAN llegue con el menor número de saltos a los servidores, tomando en cuenta que la relación más común es cliente – servidor.

No existe redundancia en las conexiones de red o backbone, por lo tanto la actual red no ofrece un buen grado de confiabilidad. Además, no se aprovechan las capacidades de los switches multilayer Cisco 3550.

En conclusión, no existe ninguna jerarquía de funciones, en la actual red de La Matriz.

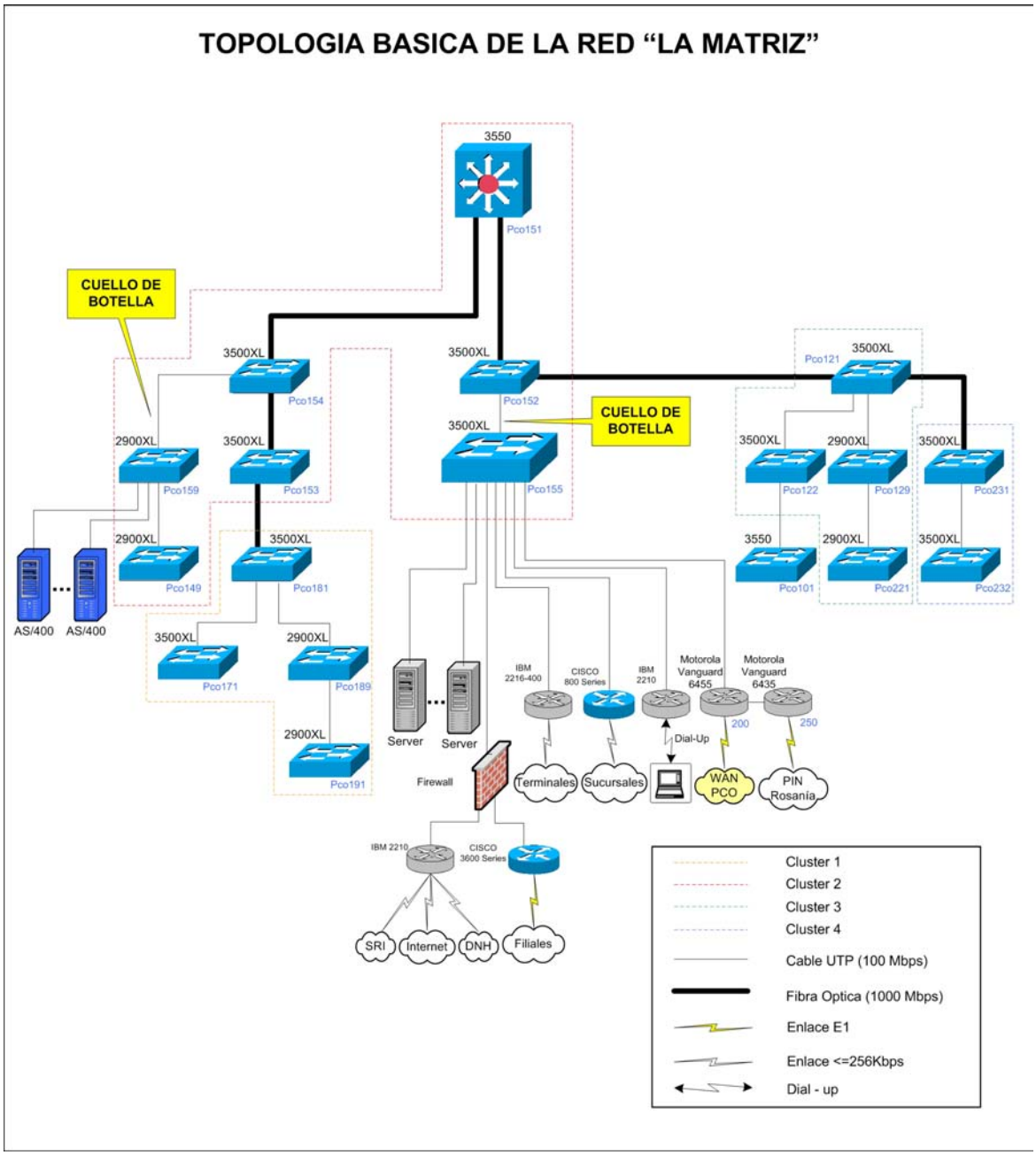


Figura 3.1 Análisis de la Topología Básica en la Red de la Matriz

3.1.2 Disposición de equipos

Tomando en cuenta que la nueva red solo va a estar conformada por Switches Cisco, se considera la siguiente información:

En la red actual se dispone de los siguientes equipos Cisco:

Cant.	Equipo	Modelo
2	Cisco Catalyst 3550 Series	WS-3550-24-PWR-SMI
10	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN
4	Cisco Catalyst 2900 XL Series	WS-C2924-XL-EN
2	Cisco Catalyst 2900 XL Series	WS-C2912-XL-EN
12	Tarjetas 1000 Base-SX Short WavelengthGBIC (multimode only)	WS-G5484

Tabla 3.1 Equipos Cisco Disponibles en la Red de la Matriz

Los nuevos equipos que se adquirieron son:

Nuevos equipos Cisco para la red futura:

Cant.	Equipo	Modelo
1	Cisco Catalyst 4500 Series	WS-C4507R
4	Tarjetas 1000 Base-SX Short WavelengthGBIC (multimode only)	WS-G5484
6	Tarjetas 1000 Base-T GBIC	WS-G5483
2	Catalyst 4500 Power over Ethernet 10/100 Base-T 48 ports (RJ-45)	WS-X4248-RJ45V
1	Catalyst 4500 Enhanced 10/100/1000 Base-T 48 ports (RJ-45)	WS-X4548-GB-RJ45
2	Catalyst 4500 Gigabit Ethernet Module 6 ports (GBIC)	WS-X4306-GB
2	Catalyst 4500 2800W AC Power Supply with Inline Power	PWR-C45-2800ACV
1	Catalyst 4507 Supervisor IV console RJ45 mgt RJ45	PWR-C45-2800ACV
1	Cisco IOS BASIC L3 Cat 4500 Sup 2+4/5.3 Des(RIP,ST, RTS,IPX,AT)	PWR-C45-2800ACV/2
2	Cisco Catalyst 3550 Series	WS-3550-24-PWR-SMI
4	Tarjetas 1000 Base-SX Short WavelengthGBIC (multimode only)	WS-G5484

Tabla 3.2 Nuevos Equipos Cisco Adquiridos

Es decir los equipos que tenemos a disposición, (sin considerar los switches Cisco 2900 XL que van a ser reubicados en otras redes), son:

Total de Equipos disponibles a ser considerados en el diseño de la nueva red

1	Cisco Catalyst 4500 Series	WS-C4507R	144
4	Cisco Catalyst 3550 Series	WS-3550-24-PWR-SMI	96
10	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN	240
		Total de Ptos diponibles:	**480**
		Total de Ptos necesarios:	**338**

20	Tarjetas 1000 Base-SX Short WavelengthGBIC (multimode only)	WS-G5484
6	Tarjetas 1000 Base-T GBIC	WS-G5483

Tabla 3.3 Total de Equipos Disponibles para el Nuevo Diseño de Red

3.1.3 Cableado y Distribución de Usuarios

Considerando la disposición futura de racks y de cableado horizontal, que converge a cada uno de ellos, como se muestra en la Figura 3.2, se establece la disposición de usuarios

por rack y por piso de los edificio el Rocio y Ex-Salesianos, incluso analizando el movimiento que tendrán ciertos departamentos, como se muestra en la Tabla 3.4.

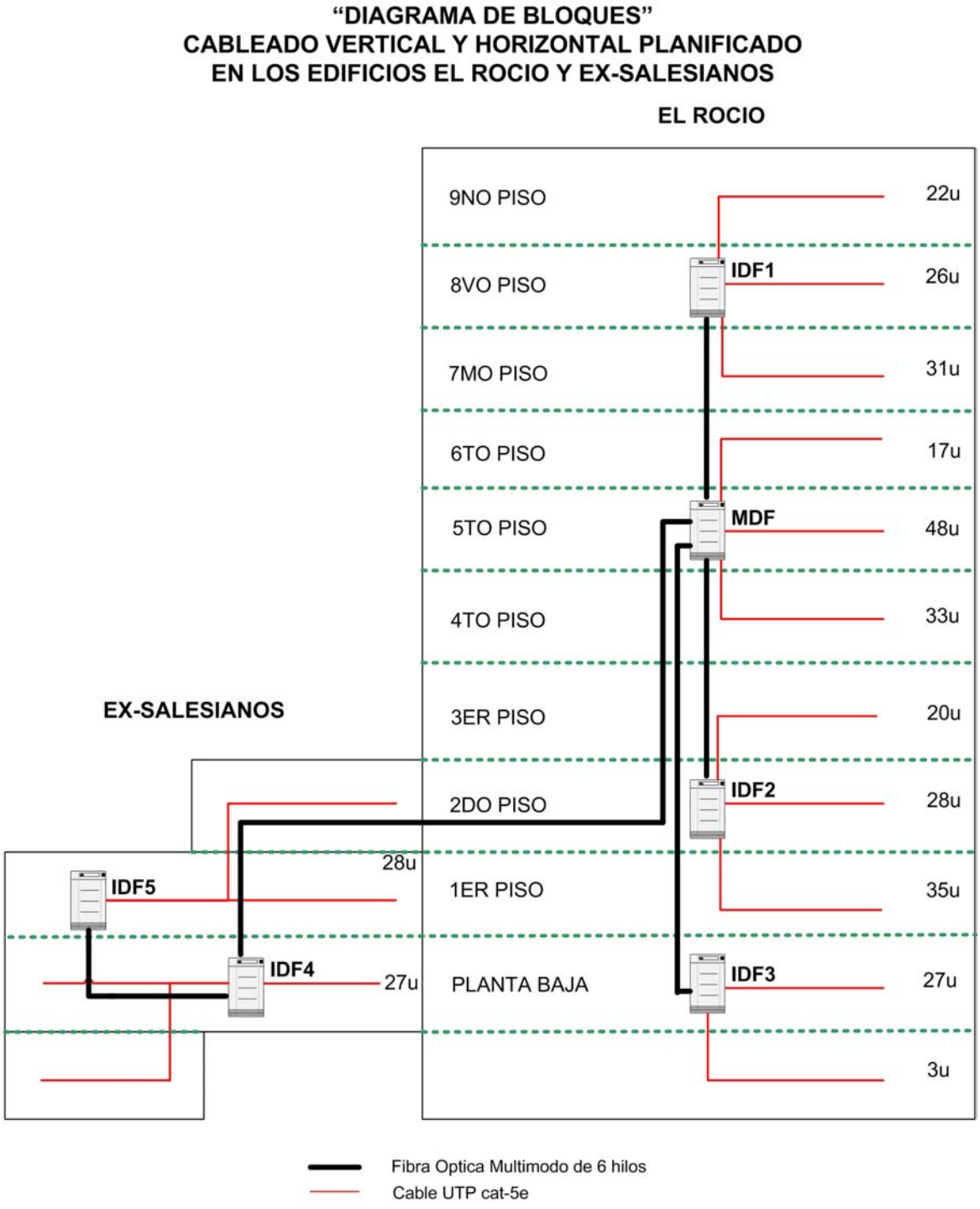


Figura 3.2 Cableado Horizontal y Vertical de la Matriz

DISTRIBUCIÓN DE USUARIIOS ACTUAL			
Piso	**Departamento**	**Usu./piso**	**Us/Rack**
9no	Legal Gerencia Norte (1 impresora+1 telf ind)	22	75
	Seguridad Física (1 equipo)		
8vo	Subgerencia de Administración y Finanzas	26	
	Recursos Humanos		
	Contabilidad (1 impresora)		
7mo	Administrativa	27	
	Servicios Administrativos (1 impresora + 1 telf ind)		
	Redes y Telecomunicaciones (1 telf ind)		
	Subgerencia de Transporte y Almacenamiento (1 imp.+ 2 telf ind)		
6to	Vicepresidencia (3 telf ind)	17	95
5to	Ingeniería y Procesamiento (15 ptos para equipos)	45	
	Redes y Telecomunicaciones (7 ptos equipos + 1 Telf ind)		
	Sistemas y Telecomunicaciones (4 impresoras + 2 telf ind)		
	Soporte Técnico y Mantenimiento (1 impresora)		
4to	Soporte de aplicaciones	33	
	Legal Vicepresidencia		
	Planificación y Finanzas		
	Programación		
3er	Subgerencia de Comercialización	20	83
	Gerencia Regional Norte		
	Comercializadora (1 impresora)		
2do	Abastecedora (con 2 impresoras)	28	
	Finanzas (1 telf ind)		
	Presupuesto (1 impresora + 1 telf ind)		
1er	Administración de Negocios Propios	35	
	Crédito y Cobranzas (1 telf. ind.)		
	Seguros y Garantías		
	Materiales		
PB	Secretaría General (1 telf ind)	27	30
	Administración de Activos		
	Administración Financiera (2 telf. Ind.)		
	Cuentas por Pagar		
	Servicios Administrativos (Recepción Rocio)		
Sub	Servicios Administrativos (Mtto. Eléctrico)	3	
	Cajita de PCO		
2do	Relaciones Públicas (1 telf ind)	15	28
	Control de Gestión (VCP) (3 telf ind)		
	Control de Gestión (VGN)		
1er	Coordinación de Contratos (1 impresora)	13	
	Bienestar Laboral (2 telf ind.)		
PB	Proyectos (1 telf ind)	8	27
	Fondo de Jubilación Especial	19	
	Proyectos		
	Soporte Técnico y Mantenimiento (1 impresora)		
	Servicios Administrativos-Recepción (1 telf ind)		
		338	338

DISTRIBUCIÓN DE USUARIIOS FUTURA			
Piso	**Departamento**	**Usu./piso**	**Us/Rack**
9no	Legal Gerencia Norte (1 impresora+1 telf ind)	22	73
	Seguridad Física (1 equipo)		
8vo	Subgerencia de Administración y Finanzas	20	
	Recursos Humanos		
	Servicios Administrativos (1 impresora + 1 telf ind)		
7mo	Administrativa	31	
	Materiales		
	Subgerencia de Transporte y Almacenamiento (1 imp.+ 2 telf ind)		
6to	Vicepresidencia (3 telf ind)	17	98
5to	Ingeniería y Procesamiento (15 ptos para equipos)	48	
	Redes y Telecomunicaciones (7 ptos equipos + 2Telf ind)		
	Sistemas y Telecomunicaciones (4 impresoras + 2 telf ind)		
	Soporte Técnico y Mantenimiento (1 impresora)		
4to	Soporte de aplicaciones	33	
	Legal Vicepresidencia		
	Planificación y Finanzas		
	Programación		
3er	Subgerencia de Comercialización	20	82
	Gerencia Regional Norte		
	Comercializadora (1 impresora)		
2do	Abastecedora (con 2 impresoras)	28	
	Finanzas (1 telf ind)		
	Presupuesto (1 impresora + 1 telf ind)		
1er	Administración de Negocios Propios	34	
	Crédito y Cobranzas (1 telf. ind.)		
	Seguros y Garantías		
	Contabilidad (1 impresora)		
PB	Secretaría General (1 telf ind)	27	30
	Administración de Activos		
	Administración Financiera (2 telf. Ind.)		
	Cuentas por Pagar		
	Servicios Administrativos (Recepción Rocio)		
Sub	Servicios Administrativos (Mtto. Eléctrico)	3	
	Cajita de PCO		
2do	Relaciones Públicas (1 telf ind)	15	28
	Control de Gestión (VCP) (3 telf ind)		
	Control de Gestión (VGN)		
1er	Bienestar Laboral (2 telf ind.)	13	
	Coordinación de Contratos (1 impresora)		
PB	Proyectos (1 telf ind)	8	27
	Fondo de Jubilación Especial	19	
	Proyectos		
	Soporte Técnico y Mantenimiento (1 impresora)		
	Servicios Administrativos-Recepción (1 telf ind)		
		338	338

Tabla 3.4 Distribución de Usuarios Futura y Actual en la Matriz

Con las dos fibras de 6 hilos entre el quinto y segundo piso, si se satisface la necesidad de 12 hilos, entre estos dos pisos, pero lamentablemente no queda ningún respaldo, por lo que se recomienda instalar otra fibra de 6 hilos entre estos dos pisos. Para obtener un diagrama unificar como se muestra en la Figura 3.3.

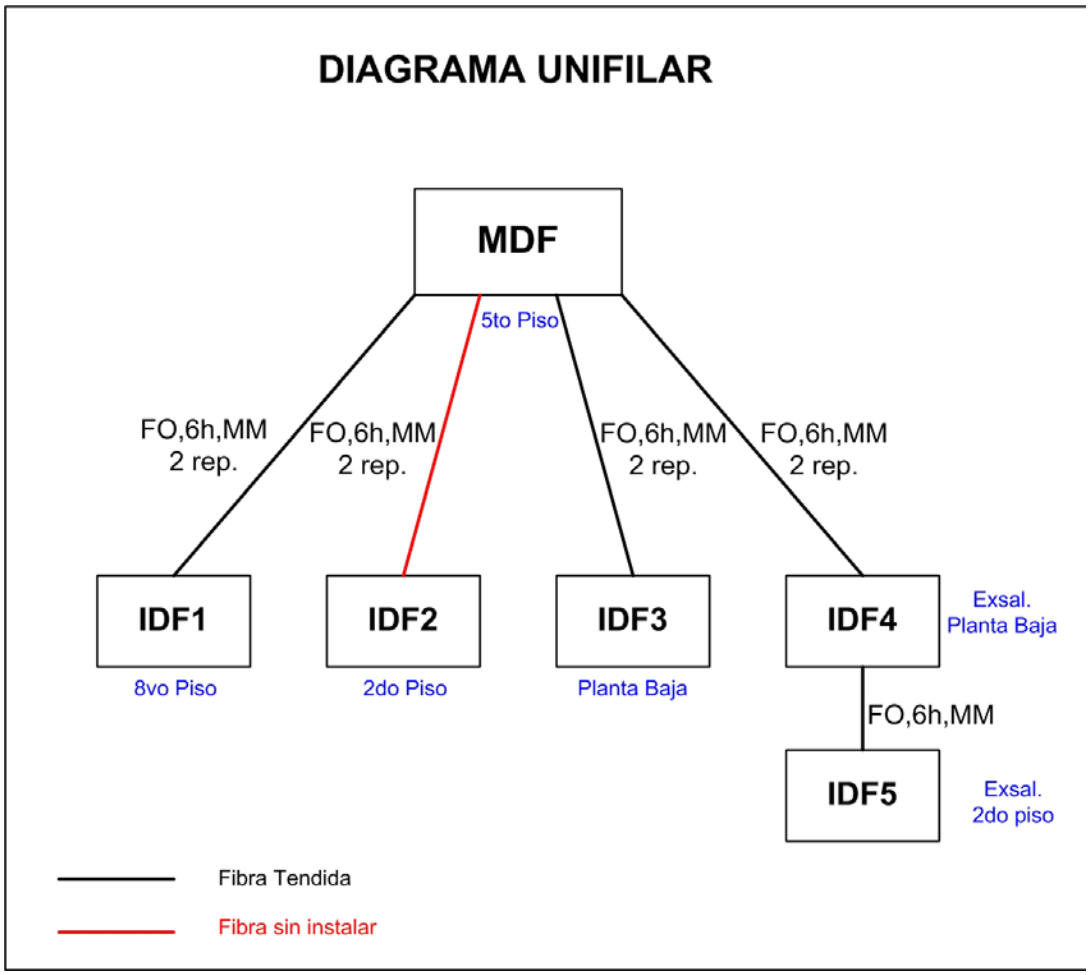


Figura 3.3 Diagrama Unifilar de la Red de la Matriz

De acuerdo a esta información se estableció la cantidad de switches mínima por rack, además de considerar que el cuarto de comunicaciones principal se adecuará en el quinto piso, por lo que definitivamente el switch de core irá ubicado en el rack de este piso y además se sugiere ubicar al menos un switch multilayer en los rack a los que convergen la mayor cantidad de usuarios.

Estableciendo así la siguiente disposición de switches por rack:

Rack del:	Cantidad de Switches	Pto Necesarios (mínimo)	Ptos Disponibles	% de Redundancia
8vo piso	1 SW 3550, 3 SW 3500XL	73	96	32 %
5to piso	1 SW 4500	98	144	47 %
2do piso	1 SW 3550, 3 SW 3500XL	82	96	17 %
La PB	1 SW 3550, 1 SW 3500XL	30	48	60 %
Exsal-PB	1 SW 3550	55	72	31 %
Exsal-1er p.	2 SW 3500XL			
	Total de puntos:	**338**	**456**	**35** %

Tabla 3.5 Disposición de Switches por Rack

Por lo tanto se tiene aproximadamente un 35% para el crecimiento de la red en general. Tomar en cuenta que todavía se puede añadir dos módulos más al switch 4500 y queda un switch 3500 XL libre, que luego puede ser ubicado de acuerdo a la necesidad.

3.1.4 Consideraciones para el Diseño de la Red de la Matriz

- Tomar como referencia el modelo jerárquico Cisco, ver en Capítulo 2, Pág. 53.
- Evitar cuellos de botella de tráfico hacia los Servidores y Sistemas AS/400 conectándolos directamente al core de la red LAN con Gigabit Ethernet, y específicamente al switch Cisco 4500 Series, para proveer un rápido manejo del tráfico IP.
- Conectar los dispositivos de la capa de distribución de los accesos a Sucursales, Terminales, Filiales y Servicios, al switch Cisco 4500 Series, para obtener un buen desempeño de la red.
- Proveer redundancia en el backbone, para dar mayor confiabilidad a la red.
- Aprovechar en su mayor capacidad, los equipos y medios que se encuentren disponibles o ya instalados (ej: switches Multicapa, Tarjetas 1000 Base-T GBIC, fibra óptica, Módulo de 6 puertos GBIC, Tarjetas 1000 Base-SX) tanto en cantidad como en eficiencia.
- Concentrar el tráfico en el switch Cisco 4500 Series por ser el switch de mayor *performance (core)*, para facilitar y centralizar la administración de la red.
- Ubicar el número necesario de switches en base a la densidad de usuarios a lo largo de los edificios El Rocio y Ex-Salesianos. Con proyección a un crecimiento aproximado del 35% de la red.

- Donde hay mayor tráfico se tratará de llegar con fibra óptica. Especialmente al rack del segundo piso, porque aquí se encuentran los usuarios que realizan las actividades más importantes para la empresa, es decir todo lo relacionado con la *Comercialización.*

Nota: El core de toda la red de Petrocomercial estaría dado por la red WAN Frame Relay, y el core de la red LAN de la Matriz, por el Switch Cisco Catalyst 4500 Series.

Nota: El objetivo principal de Petrocomercial es el transporte, almacenamiento y comercialización de derivados de petróleo en el territorio nacional.

3.1.5 Diseños Propuestos

Características generales de las Alternativas 1, 2 y 5:

- El Switch Cisco 4500 Series, trabajará en la capa de core de la red de la Matriz.
- Los Switches Cisco 3550 Series, trabajarán en la capa de distribución (se recomienda poner aquí las listas de acceso) y en la capa de acceso.
- Los Switches Cisco 3500 XL trabajarán solamente en la capa de acceso.

Características generales de las Alternativas 3,4 y 6:

- El Switch Cisco 4500 Series, trabajará en la capa de core, distribución y de acceso de la red de la Matriz; por su alta capacidad de procesamiento, su disponibilidad de módulos y por su prestación de funciones.
- Los Switches Cisco 3550 Series trabajarán en la capa de acceso y si es necesario también trabajarán en la capa de distribución.
- Los Switches Cisco 3500XL Series, trabajarán en la capa de acceso.

3.1.5.1 Alternativa 1

Ventajas:

- Redundancia en la capa de acceso
- Utilizo las 6 tarjetas 1000 Base-T GBIC
- Fácil de construir el backbone físico de la LAN, considerando que el backbone de fibra ya está tendido.
- La disposición de medios (fibra) es adecuada porque generalmente estas son las rutas que tomará el tráfico, de acuerdo al presente diseño.
- Existe concentración directa de tráfico al swtich de core

Desventajas:

- El tráfico desde los extremos del backbone (capa de acceso), hacia los servidores y AS400's tiene un considerable número de saltos, tomando en cuenta que la relación más común es cliente – servidor.
- No se aprovechan todos los hilos de fibra óptica multimodo ya tendidos.

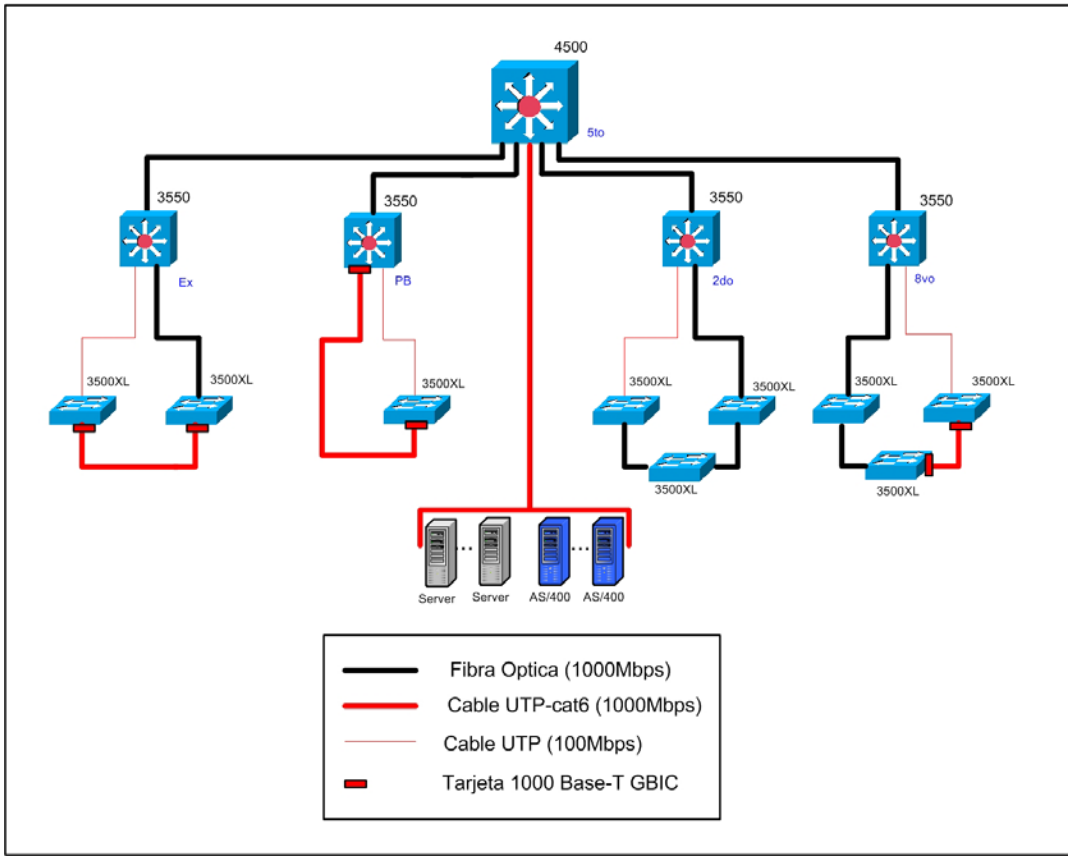


Figura 3.4 Diseño de Red de la Alternativa 1

3.1.5.2 Alternativa 2

Ventajas:

- Redundancia en la capa de acceso
- Redundancia en la capa de distribución (mayor confiabilidad)
- Utilizo las 6 tarjetas 1000 Base-T GBIC
- Fácil de construir el backbone físico de la LAN, considerando que el backbone de fibra ya está tendido.
- La disposición de medios (fibra) es adecuada porque generalmente estas son las rutas que tomará el tráfico, de acuerdo al presente diseño.
- Existe concentración directa de tráfico al swtich de core

Desventajas:

- Dificultad en tender cable UTP, desde la planta baja del Rocio a la planta baja de Ex-Salesianos y del 2do piso al 8vo piso en el edificio el Rocio.
- El tráfico desde los extremos del backbone (capa de acceso), hacia los servidores y AS400's tiene un considerable número de saltos, tomando en cuenta que la relación más común es cliente – servidor.
- No se aprovechan todos los hilos de fibra óptica multimodo ya tendidos.

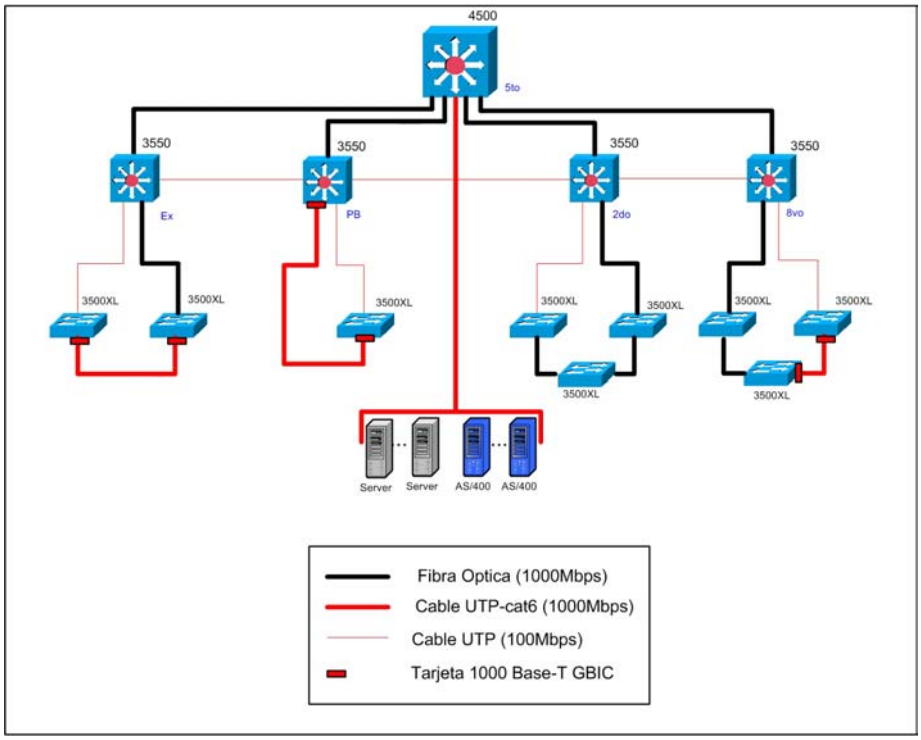


Figura 3.5 Diseño de Red de la Alternativa 2

3.1.5.3 Alternativa 3

Ventajas:

- Redundancia en el backbone de la red
- Utilizo 5 tarjetas 1000 Base-T GBIC
- El backbone físico de fibra para este diseño ya está tendida.
- Existe concentración directa de tráfico al swtich de core
- Se tiene más rutas alternas para llegar al core sin necesidad de dar muchos saltos entre switches, tomando en cuenta que la relación más común es cliente – servidor, y los servidores están directamente conectados al Switch 4500.
- Se aprovechan y se puede continuar aprovechando en mayor cantidad, los hilos de fibra óptica multimodo ya tendidos.

Desventajas:

- Dificultad en tender el backbone 1000 Base-T con cable UTP cat 6 desde el 8vo al 5to piso.

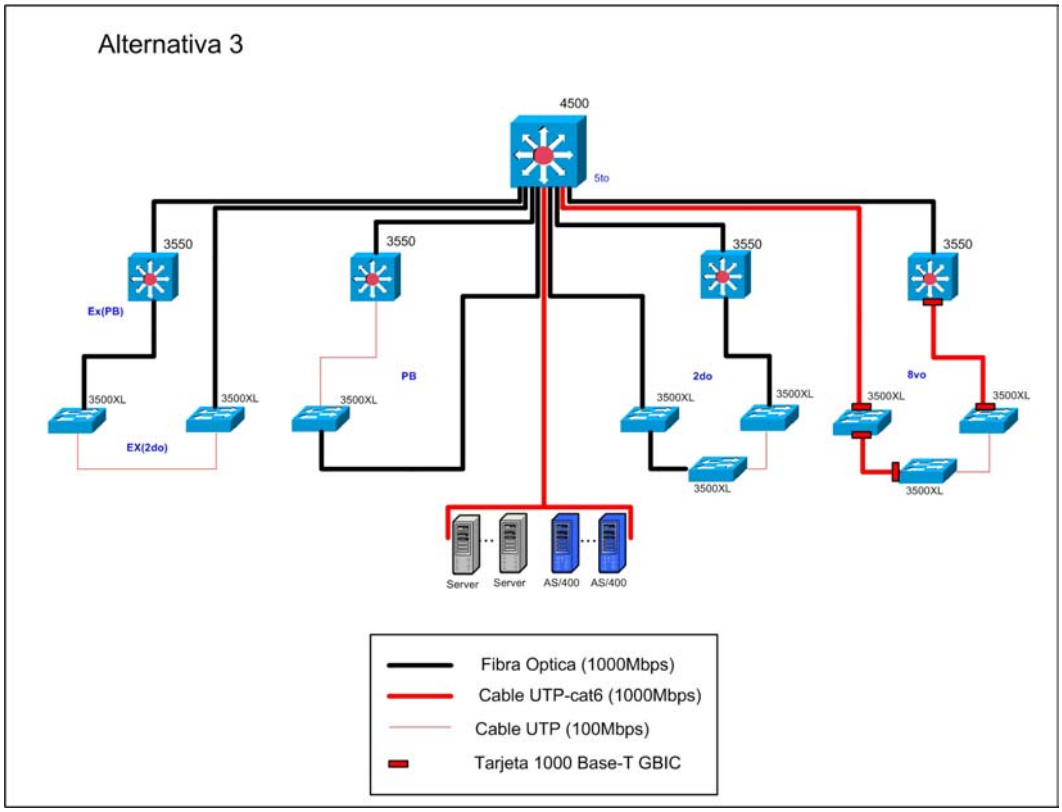


Figura 3.6 Diseño de Red de la Alternativa 3

3.1.5.4 Alternativa 4

Ventajas:

- Mayor redundancia en el backbone de la red que la alternativa 3
- Utilizo 5 tarjetas 1000 Base-T GBIC
- El backbone físico de fibra para este diseño ya está tendida.
- Existe concentración directa de tráfico al swtich de core.
- Se tiene más rutas alternas para llegar al core sin necesidad de dar muchos saltos entre switches, tomando en cuenta que la relación más común es cliente – servidor, y los servidores están directamente conectados al Switch 4500.
- Se aprovechan y se puede continuar aprovechando en mayor cantidad, los hilos de fibra óptica multimodo ya tendidos.

Desventajas:

- Dificultad en tender el backbone 1000 Base-T con cable UTP cat 6 desde el 8vo al 5to piso.
- También hay dificultad en tender cable UTP, desde la planta baja del Rocio a la planta baja de Ex-Salesianos y desde del 2do al 8vo piso en el edificio el Rocio.

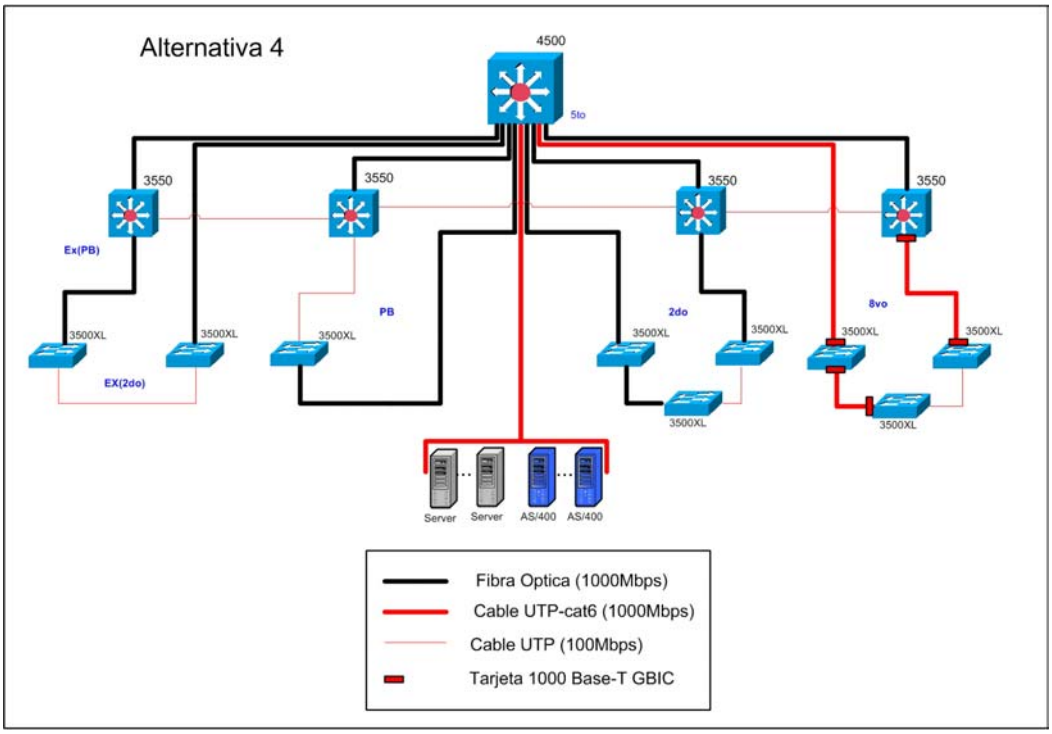


Figura 3.7 Diseño de Red de la Alternativa 4

3.1.5.5 Alternativa 5

Ventajas:

- Redundancia en la capa de distribución con fibra.

Desventajas:

- Dificultad en tender fibra del 2do al 8vo piso.
- Los medios (fibra) no concuerdan con el comportamiento normal del tráfico
- No llego con fibra hasta los puntos de acceso donde hay más tráfico
- Desperdicio fibra tendida al edificio de Ex-Salesianos

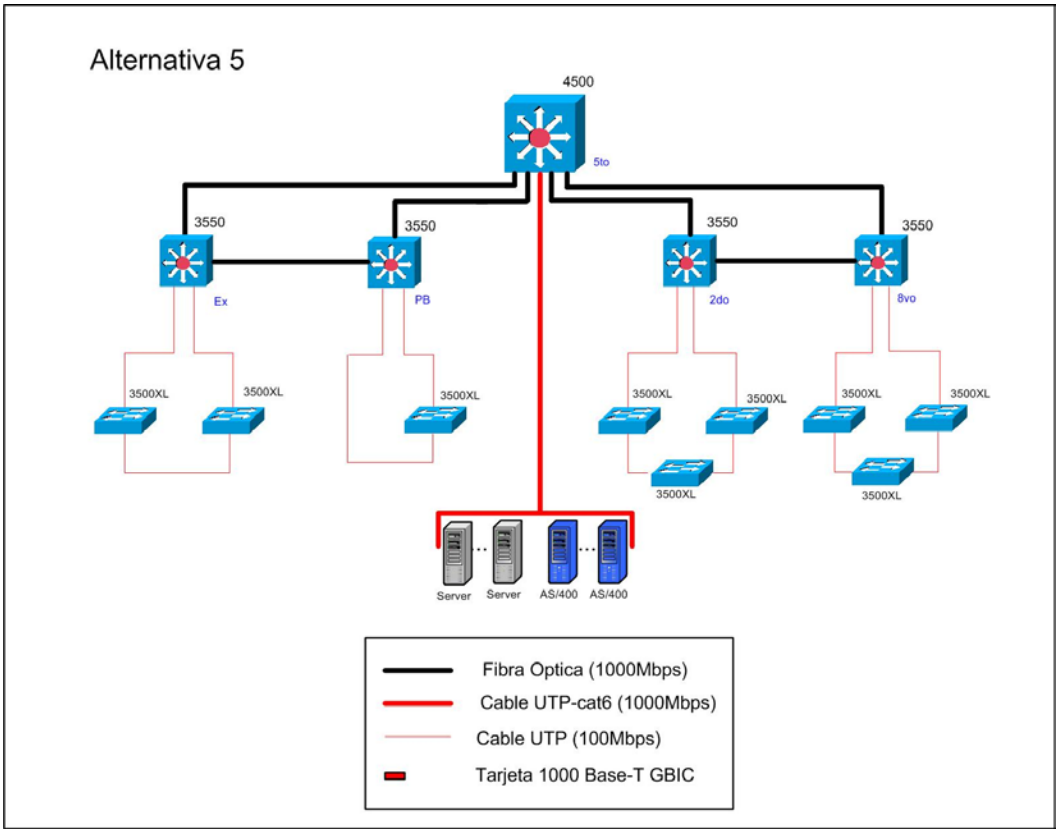


Figura 3.8 Diseño de Red de la Alternativa 5

3.1.5.6 Alternativa 6

Ventajas:

- Mayor redundancia en la capa de distribución con fibra.
- Utilizo las 6 tarjetas 1000 Base-T GBIC
- Existe concentración directa de tráfico al swtich de core
- Existen más rutas alternas para llegar al core sin necesidad de dar muchos saltos entre switches, tomando en cuenta que la relación más común es cliente – servidor.

Desventajas:

- La disposición del backbone de fibra no concuerda con el comportamiento normal del tráfico.
- En los caminos redundantes existe mucha inversión, cuando debería utilizarse simplemente un medio menos costoso, como cable UTP en lugar de fibra ótica.
- Dificultad en tender fibra del 2do al 8vo piso y de la planta baja del Rocio a la planta baja de Ex-Salesianos.

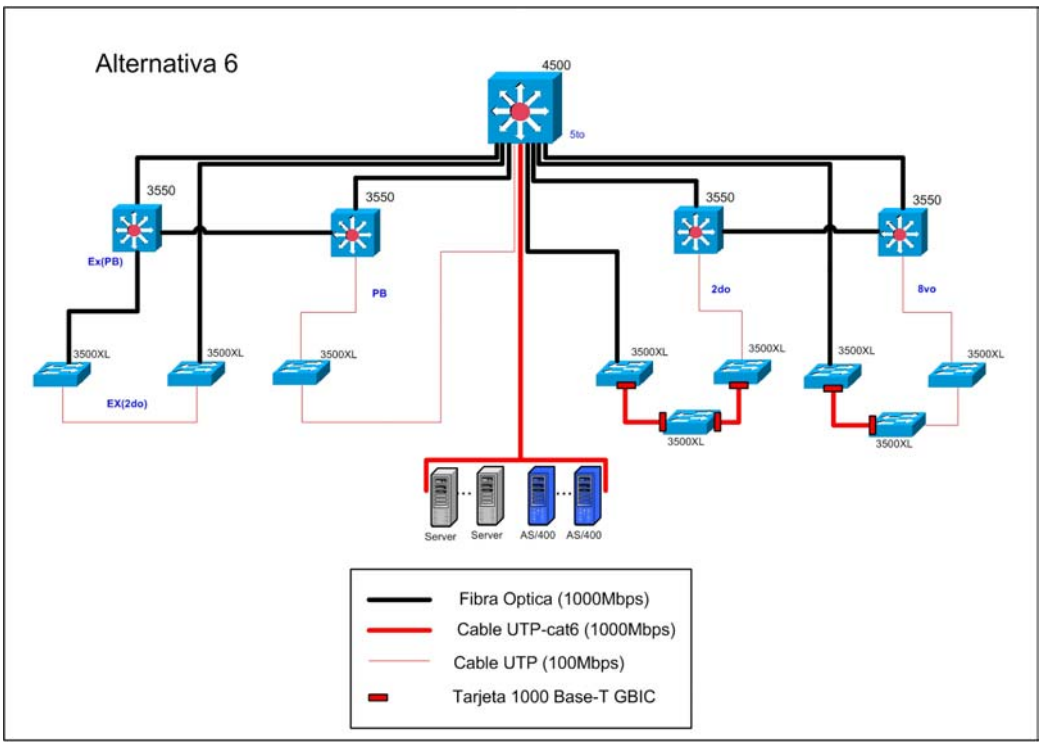


Figura 3.9 Diseño de Red de la Alternativa 6

3.1.6 Elección del Mejor Diseño de Red

Tomando en cuenta las consideraciones de diseño antes ya mencionadas, las 2 mejores propuestas son: la Alternativa 3 y la Alternativa 4, principalmente porque ofrecen una mayor centralización del flujo de tráfico lo cual facilita la administración y control del mismo, además que aprovechan de mejor forma los principales medios disponibles es decir la fibra óptica.

La única diferencia entre la alternativa 3 y la alternativa 4, son los tres tramos de redundancia (backup) con cable UTP entre los switches del 2do, 8vo, planta baja (del edificio Rocio) y 2do piso del edificio Ex-Salesianos. Y tomando en cuenta que la redundancia que se tiene con cada uno de los anillos hacia cada uno de los cuartos de distribución es suficiente, se eligió como mejor opción la **ALTERNATIVA 3,** ver Figura 3.10.

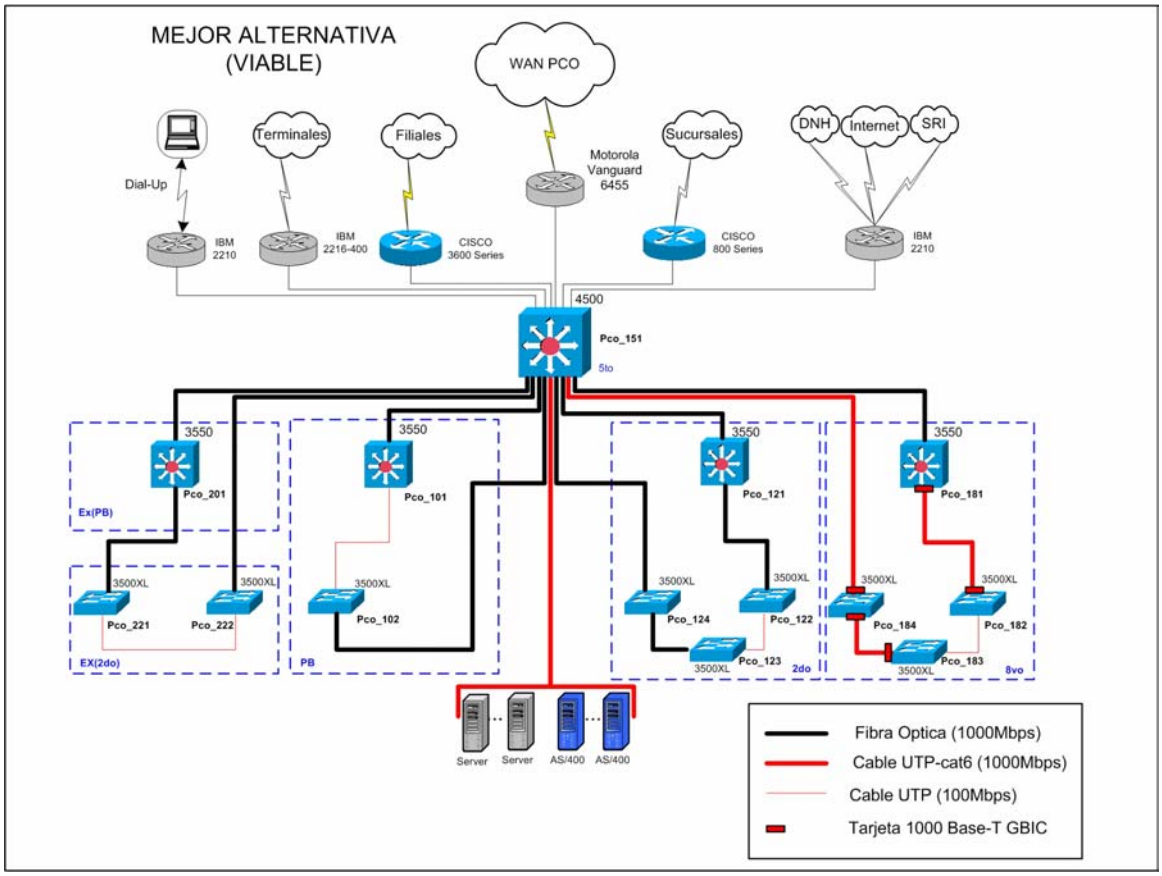


Figura 3.10 Diseño de Red de la Mejor Alternativa

Para conseguir el backbone de este diseño se necesita tender cable UTP cat-6 o cat-5e desde el quinto al octavo piso del Edificio el Rocio.

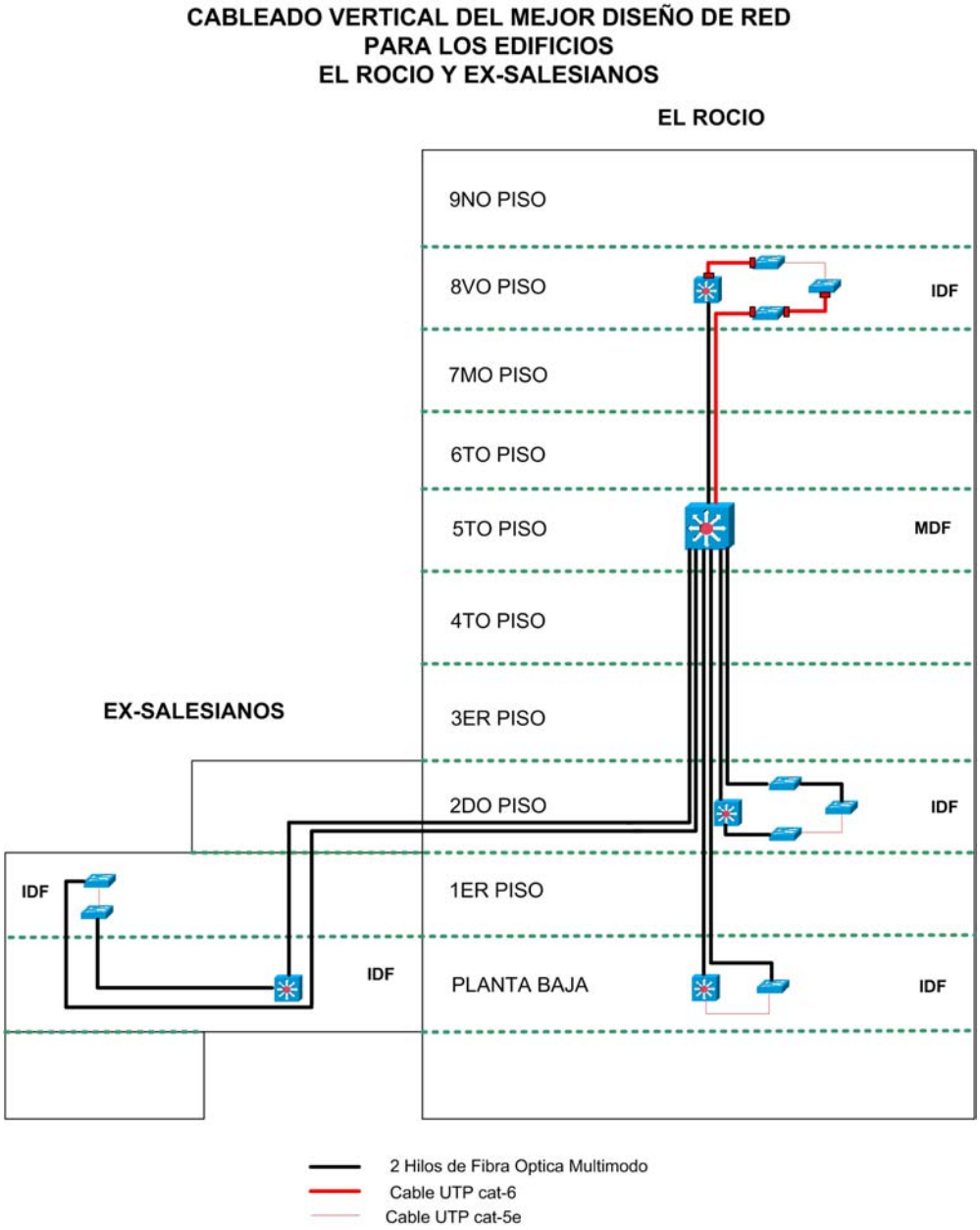


Figura 3.11 Cableado Vertical del Mejor Diseño de Red

Para realmente tener un backbone sumamente robusto y aprovechar de forma completa los recursos tales como: el número de hilos de fibra óptica ya tendida (sin descuidar hilos de fibra para respaldo, "backup"), las tarjetas 1000 Base-SX, las tarjetas 1000 Base-T GBIC, y los dos módulos GBIC del Supervisor Engine IV del Cisco Catalyst 4500 Series. Se propone el mismo diseño con ciertas mejoras que definitivamente la convierten en la mejor elección, consiguiendo llegar a todos los switches con fibra óptica y

cerrar los anillos incompletos con 1000 Base-T. Para así finalmente formar un backbone de fibra óptica complementado con cable UTP cat-6 a 1000 Mbps. Como se muestra en la Figura 3.12.

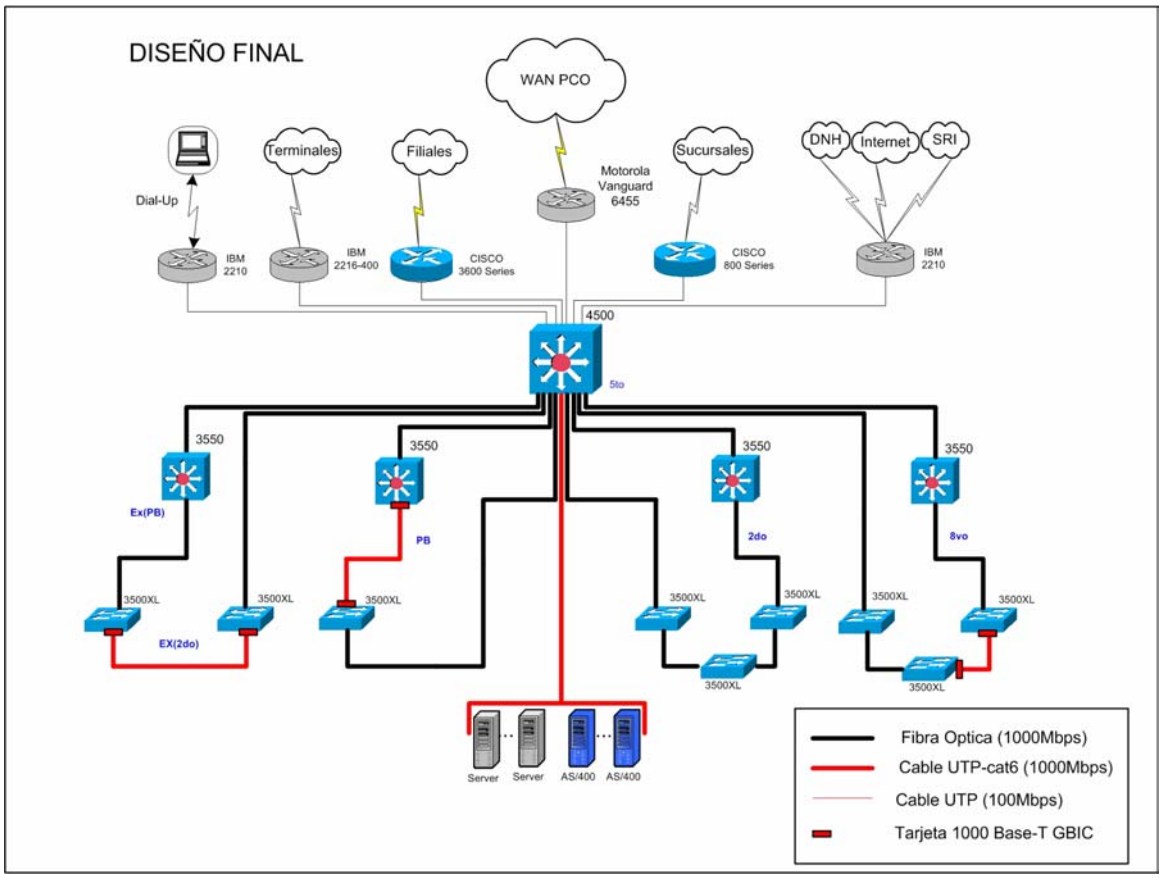


Figura 3.12 Diseño Final Propuesto

Además, otra ventaja que ofrece este diseño va a ser la facilidad de administración porque gracias a los modelos de switches que se están utilizando y a la distribución de éstos, a lo largo de la red, se pueden construir cuatro clusters, uno por cada rack, (excepto para Ex-Salesianos, quienes tendrán un solo cluster), que a través del programa Cluster Managment Suite, nos ayudará en la configuración y administración de estos switches; excepto el switch 4500, que no soporta esta aplicación.

Para conseguir este objetivo se necesita:

- Comprar 8 Tarjetas Cisco 1000 Base-SX Short Wavelength GBIC (multimode only) WS-G5484.

Nota: Se recomienda tender fibra óptica de 6 hilos multimodo entre el quinto y segundo piso, para tener hilos de fibra de respaldo.

Obviamente los equipos con los que se cuenta actualmente, servirán para llegar al Diseño seleccionado como "Mejor Alternativa", y luego de realizar la compra de las ocho tarjetas 1000 Base-SX se escalará al "Diseño Final" propuesto. Además se debe tomar en consideración que si se realiza la compra de tarjetas Gigabit Ethernet para los servidores, y para fibra óptica, será necesario la compra de un módulo de puertos GBIC para el Swtich Cisco 4500 Series.

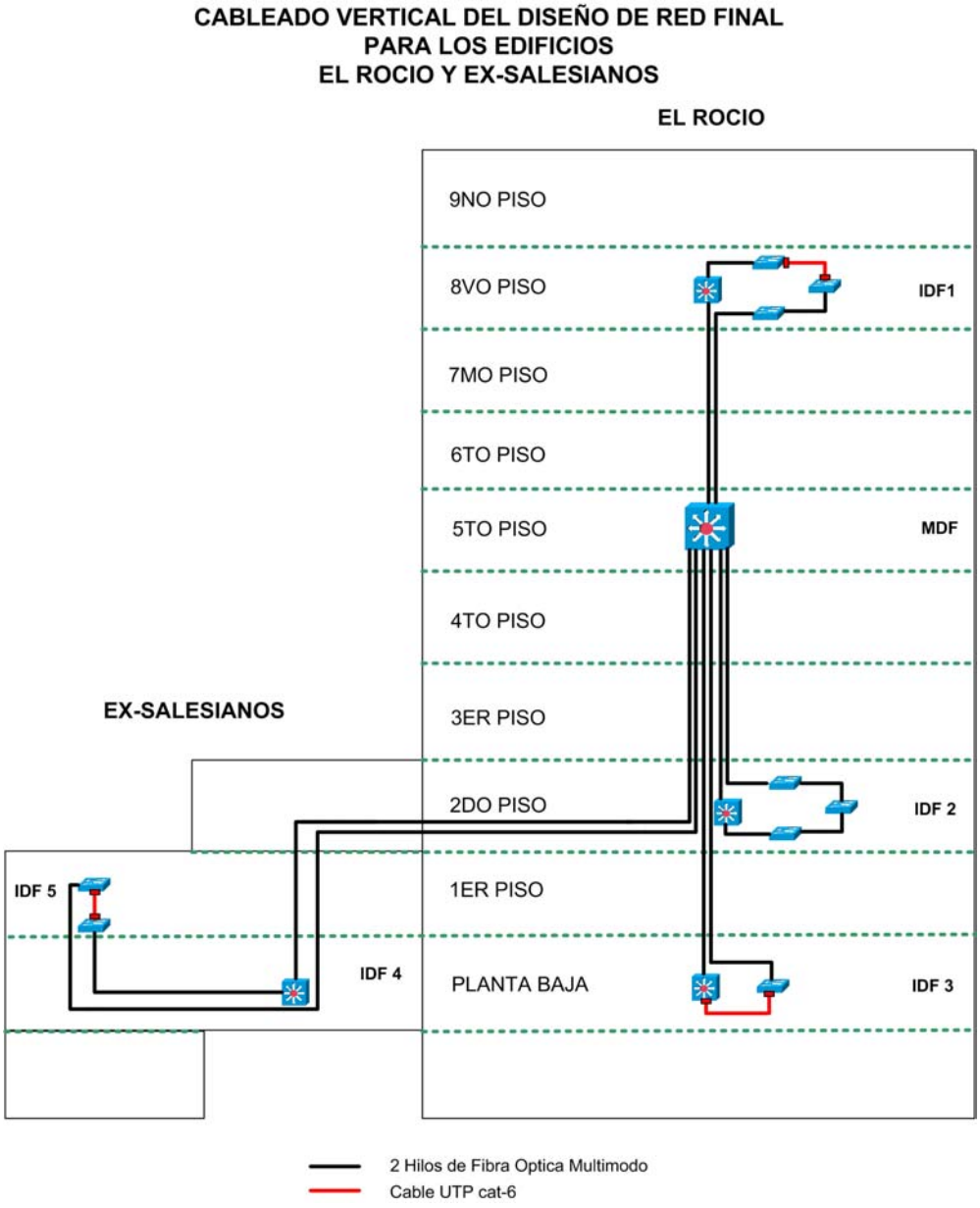


Figura 3.13 Cableado Vertical del Diseño Final Propuesto

Si el presupuesto es limitado al menos se recomienda comprar 4 de estas tarjetas 1000 Base-SX para ir y regresar con fibra a los racks del octavo piso y planta baja y no desperdiciar los hilos de fibra tendidos. Como se muestra en la Figura 3.14.

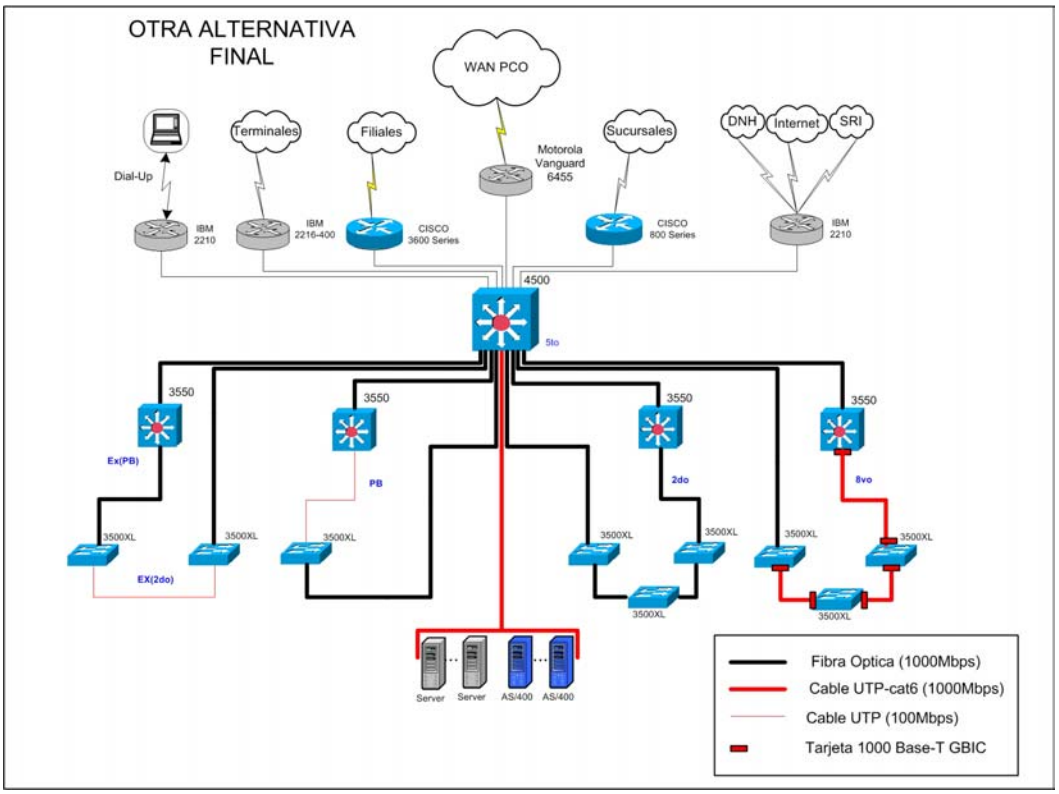


Figura 3.14 Otra alternativa a Considerar

3.1.6.1 Ventajas del Diseño Final Propuesto

Con el presente diseño recomendado basado en el modelo jerárquico Cisco se provee:

- Buen rendimiento de la red
- Escalabilidad.
- Confiabilidad.
- Facilidad de monitorear la red
- Facilidad de localizar y resolver problemas
- Facilidad de predecir el comportamiento de la red

3.1.7 Diseño de VLANs para la Red de la Matriz

A través del análisis que se ha ido desarrollado acerca del comportamiento del tráfico en la red de la Matriz, y de cómo aprovechar de mejor forma los beneficios que nos ofrecen las VLANs, se han desarrollado dos propuestas de diseño de VLANs para esta red.

3.1.7.1 Análisis de Diseños propuestos

La **primera propuesta,** (ver Figura 3.15), se considera la propuesta base para ambos diseños, porque ésta presenta el mismo número de VLANs y la agrupación de usuarios es similar a la segunda propuesta, más no la ubicación de los servidores y otras características que luego se explicarán.

En la primera propuesta, si se realiza un enfoque particular de la ubicación de los servidores, en donde radicalmente se agrupa a todos ellos en una sola VLAN, esto no es lo más apropiado, como se observa en la Figura 3.15, porque definitivamente todos los usuarios que pertenecen a las otras VLANs que es más del 85% de la red de la Matriz, deberán realizar enrutamiento para llegar a la VLAN donde se encuentran estos servidores, lo cual implica a su vez que se incrementa la latencia[1] de los paquetes porque estos son analizados hasta capa 3, y obviamente no estamos aprovechando la principal característica que nos ofrece las VLANs, que es el de mejorar el desempeño de la red, agrupando de forma adecuada las estaciones de trabajo con los servidores que estos utilizan, es decir no se está segmentando adecuadamente los dominios de broadcast creados por estas VLANs. Por lo tanto con esta primera propuesta no se va a ver una mejoría en el desempeño de la red.

También cierto es, que no se tiene por cada grupo de trabajo de la empresa un solo servidor, lo cual sería lo ideal, pero no por ello se debe asumir que todos los servidores son servidores empresariales[2].

Y aunque la fortaleza de esta primera propuesta al parecer es la seguridad, es claro que a nivel del switch multilayer Cisco Catalyst 4507R esto debe realizarse a través de listas de a acceso, lo cual también es factible con la segunda propuesta.

[1] Latencia: es el tiempo que demora un paquete en viajar desde su origen a su destino.
[2] Servidores empresariales: Son servidores con aplicaciones que dan servicio a toda empresa.

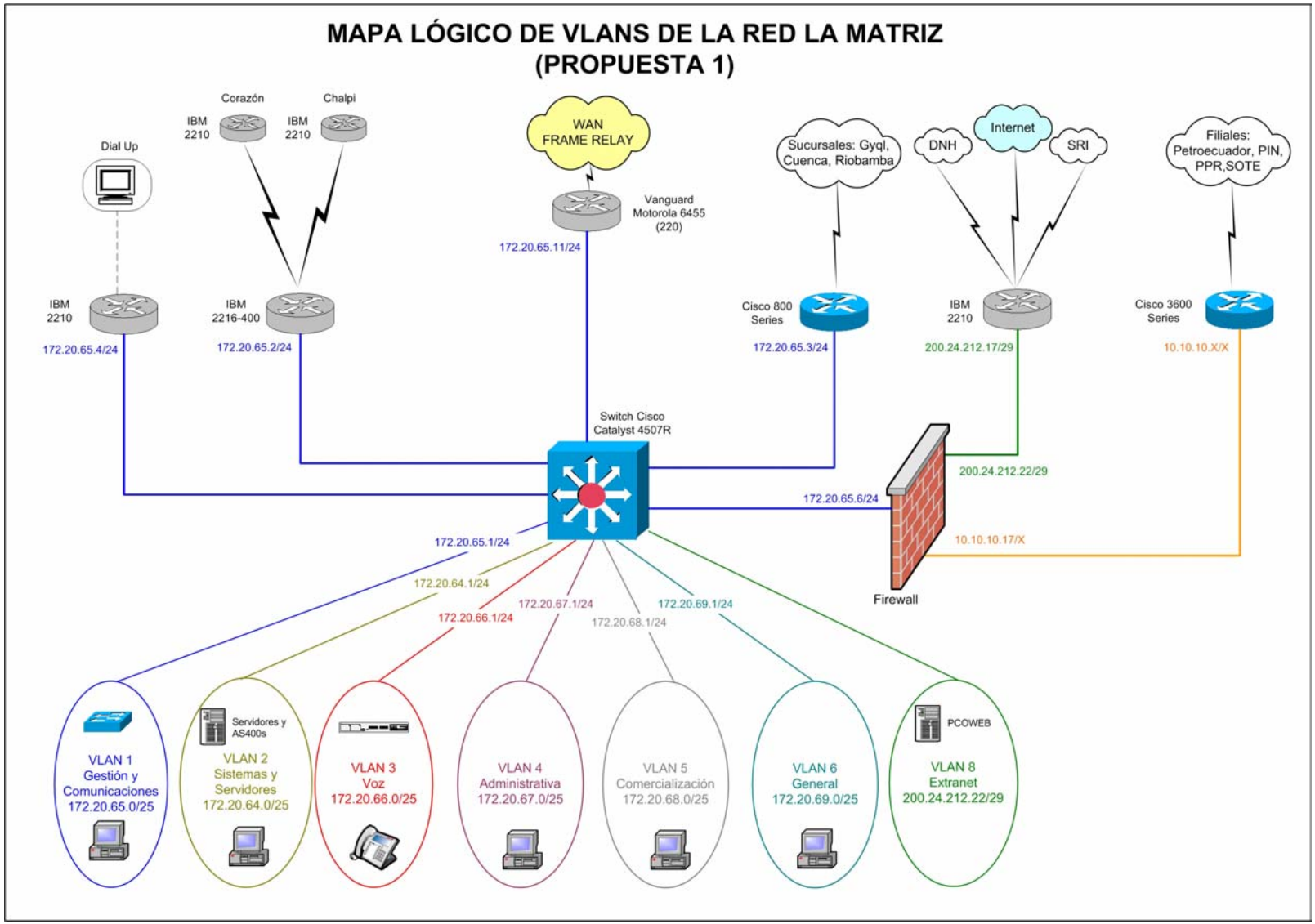


Figura 3.15 Mapa Lógico de VLANs para la Red de la Matriz 1

Otra característica de esta primera propuesta, es que todas las interfaces LAN de los routers que ofrecen los diferentes accesos, son parte de la VLAN de Gestion de Red, es decir de la VLAN 1 que es la que administra todos los equipos de interconexión de red. Lo que a su vez indica que los puertos del Switch Cisco 4507R son puertos conmutados (*switch ports*) o puertos de capa 2 que serán configurados como puertos de acceso a la VLAN 1. Esto implica que los broadcast generados por la VLAN 1 también van a llegar hasta las interfaces LAN de los routers, por lo tanto se está consumiendo de forma innecesaria el ancho de banda de estos accesos y recursos de estos dispositvos. Otro punto negativo a que las interfaces LAN de los routers formen parte de la VLAN 1, es que las seguridades que se puedan implementar sobre el switch Cisco 4507R serán limitadas o no serán las mejores, porque por ejemplo en el caso de utilizar VLAN maps[1], éstas interferirán con el desempeño de toda la VLAN 1. Por lo tanto con esta primera propuesta no se pueden implementar seguridades hacia los routers de acceso. Tomar muy en cuenta esto, porque además, no se tiene ningún tipo de filtrado en estos equipos.

A partir de las falencias identificadas en la primera propuesta, surge otra mejorada, tratando de corregir estos errores y aprovechar de mejor forma los beneficios de las VLANs, especialmente para que mejore el desempeño de la red y con una proyección viable de seguridad a los accesos remotos.

En la **segunda propuesta,** (ver Figura 3.16)**,** a partir del mismo análisis que se realizó en la primera propuesta, para ver que servidores utiliza cada departamento, (ver Tabla 3.6), se puede observar claramente que existen 3 flujos de tráfico, que resultan del acceso de las máquinas a los siguientes grupos de servidores:

- PCO1, PCO2 y PCORED4 (PCORED5 backup)
- PCO8 Y PCO9
- PCORED, PCORED1 y PECORED7

Por lo tanto, con esta información y conociendo las aplicaciones que corren en cada uno de los servidores (Ver Anexo 1), se puede concluir, que si se pueden definir Servidores de Grupo de Trabajo que son: el primer grupo conformado por: PCO1, PCO2, PCORED4,

[1] VLAN Maps son listas de acceso que pueden filtrar tráfico entre dispositivos dentro de la misma VLAN o filtrar paquetes que van hacia fuera o hacia dentro de una VLAN.

y PCORED5 y el otro grupo formado por: PCO8 y PCO9; mientras que los Servidores Empresariales son: PCORED, PCORED1 y PECORED7. Es decir, estas definiciones determinan que la ubicación adecuada de estos grupos de servidores, debe ser en sus respectivas VLANs, y no en una sola, como lo propone el primer diseño.

Esto quiere decir que en la red de la Matriz, se va a trabajar con la regla de flujo de tráfico 80/20, al menos en las VLANs que poseen sus propios servidores de grupo de trabajo, es decir son VLANs *end-to-end*; mientras que las VLANs que no tengan sus propios servidores, son VLANs Geográficas, que significa que el 20 por ciento del tráfico se mantiene dentro de la VLAN local y el 80 por ciento del tráfico de la red viaja fuera de ella. Por lo tanto esta nueva ubicación de servidores si mejora el desempeño de la red, y más aun, si recordamos que la relación más común dentro de la empresa, es el relación cliente – servidor. Esta es otra razón por la cual se pone tanto empeño en la ubicación de los servidores.

Otra mejora de esta propuesta de diseño, está en la configuración de puertos enrutados en lugar de puertos conmutados, hacia las interfaces LAN de los routers que proveen los diferentes accesos, y del Firewall que filtra los paquetes que llegan desde otras Filiales o de la extranet en general. Característica que provee una mejor proyección de seguridad hacia los routers de acceso y una adecuada segmentación del dominio de broadcast de la VLAN 1, que anteriormente estaba mal distribuido.

Según los argumentos expuestos, la segunda propuesta es el mejor diseño de VLANs, pero la razón por la cual todavía se toma en cuenta a la primera propuesta, es porque está ofrece mayor facilidad en la implementación, especialmente en lo que se refiere al cambio de direccionamiento, porque esta solo requiere fundamentalmente el cambio de las direcciones de las interfaces LAN de los routers y del servidor PCORED1, mientras que la segunda propuesta requiere tanto el cambio de las direcciones de todos los servidores y AS400s como de las interfaces LAN de los routers, es decir es un cambio radical del direccionamiento de toda la red de la Matriz. Es por esta razón que si la empresa desea elegir el primer diseño, por la facilidad de implementación ateniéndose a las limitaciones ya explicadas, la información necesaria de la primera propuesta está disponible en el Anexo 9, pero debido a que la segunda propuesta definitivamente es la mejor, entonces se decidió por trabajar con éste diseño y a continuación se detalla el análisis del mismo.

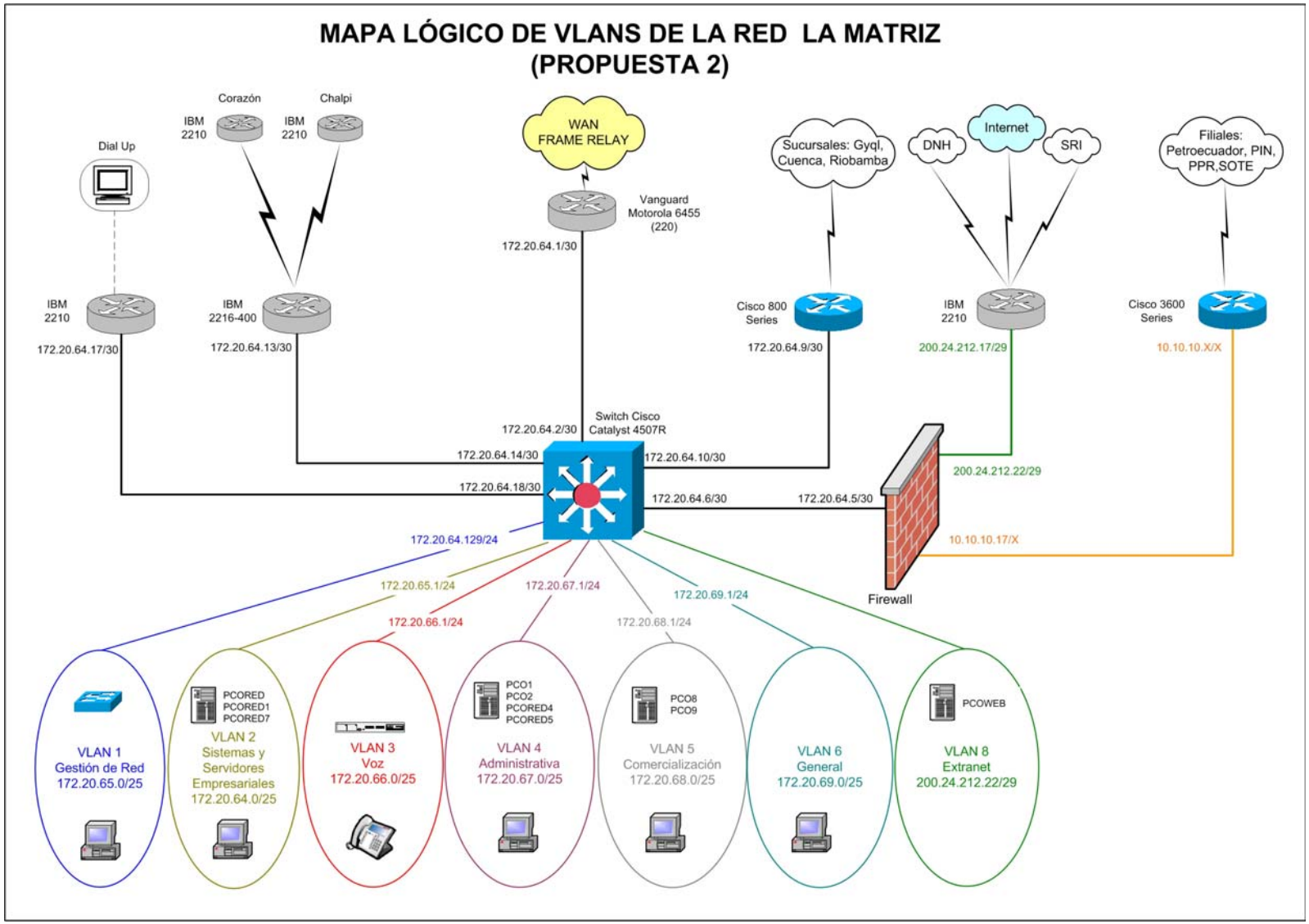


Figura 3.16 Mapa Lógico de VLANs para la Red de la Matriz 2

3.1.7.2 Desarrollo del Mejor Diseño Propuesto

Para la administración de los equipos de interconexión de red o switches y las computadoras que los administran, (usuarios de Telecomunicaciones), se utilizará la VLAN 1, que por defecto es la VLAN de administración propia de los switches, que se denominará: VLAN DE GESTION DE RED.

Los servidores empresariales estarán dentro de otra VLAN, al igual que las máquinas que los administran, es decir las computadoras de Sistemas y las máquinas controladas por el Firewall. Esta VLAN se denomina: VLAN DE GESTION DE SERVIDORES.

Nota: Para que los usuarios de la red de la Matriz se comuniquen con los servidores empresariales, necesariamente deben recurrir al enrutamiento, esto es algo inevitable debido a las funciones propias de estos servidores. Pero al menos ya no se realiza esta tarea con todos los servidores.

A la siguiente VLAN corresponden los teléfonos IP y las direcciones estáticas de la Central IP Mitel, que será conocida como la VLAN DE VOZ.

El criterio que se utilizó para agrupar los usuarios de datos a las VLANs, es de acuerdo al flujo de tráfico, es decir en base a que servidores acceden por lo general las máquinas. De esta forma, como anteriormente ya se mencionó, se determinó que existen básicamente 3 flujos de tráfico; las máquinas que acceden a:

- PCO1, PCO2 y PCORED4 (PCORED5 backup)
- PCO8 Y PCO9
- PCORED, PCORED1 y PECORED7

Los servidores PCO1, PCO2 y PCORED4, tienen aplicaciones de Recursos Humanos, Contratos, Contabilidad, Movimiento de productos, *DataWareHouse*, *Bussiness Object*, etc; es decir aplicaciones orientadas a la Administración por lo que a esta VLAN se le asignó el nombre de VLAN ADMINISTRATIVA.

Nota: El PCORED5 forma también parte de la VLAN ADMINISTRATIVA porque éste es un servidor de respaldo del PCORED4.

Los servidores PCO8 y PCO9, manejan aplicaciones de Comercialización Interna, Movimiento de Productos, Base de datos de Comercialización Interna, etc.; por lo tanto son aplicaciones dedicadas al área de Comercialización de Petrocomercial, razón por la cual esta VLAN tiene el nombre de VLAN DE COMERCIALIZACION.

El tercer flujo de tráfico lo forman las máquinas que acceden a los servidores empresariales PCORED, PCORED1 y PCORED7, pero obviamente estos servidores ya tienen su propia VLAN, porque a ellos recurrirán todos los usuarios, y no es lógico agruparlos con cierto grupo de trabajo, excepto con los que los administran, como ya se determinó anteriormente.

Las aplicaciones de PCORED y PCORED1 son: Correo Interno, Órdenes de Pago, Viáticos, DHCP, DNS, DNH, SRI, Sistemas Oferentes, Auditoría, Norton Antivirus, etc; es decir son aplicaciones generales que todos los usuarios utilizan, mientras que el PCORED7 tiene como aplicación el Control Documental 2005 que generalmente lo emplean las secretarias de cada Unidad. Pero la razón por la cual el PCORED7 forma parte de los servidores empresariales principalmente es porque ciertas aplicaciones de PCORED van a pasar a este servidor en el futuro.

Si nos fijamos en la Tabla 3.6, existe un número considerable de usuarios que no utilizan un grupo de "servidores de grupo de trabajo" en particular, es decir generalmente solo recurren a los servidores empresariales, pero entonces a partir de lo ultimo mencionado, quizás surge la pregunta de porque estos usuarios no forman parte de la VLAN de los servidores empresariales, y la razón es por seguridad, porque cualquier usuario no debe tener un acceso libre a estos servidores, a menos que se lo permita. Por lo tanto a estos usuarios se les asigna otra VLAN que tiene el nombre de VLAN GENERAL.

Y finalmente las VLANs que necesariamente tienen que existir para dar mayor seguridad a la intranet son la VLAN DE FILIALES que lo constituyen las redes externas como: Petroecuador, Petroproducción, SOTE, etc., y la VLAN DE LA EXTRANET, que corresponde al Internet.

La razón por la cual los accesos a estos dos tipos de redes de Filiales y Extranet, tienen asignadas VLANs, y por ende son conectados a puertos conmutados (capa 2), en lugar de utilizar puertos enrutados (capa 3) y tratar a estos dos accesos como dos subredes

independientes, y así de igual forma poder aplicar seguridades, es porque a estos dos tipos de red se adhieren mas accesos, como por ejemplo el Servidor Web que necesita estar en la red Externa, y otras utilidades. Por lo tanto, al asignar a las Filiales y a la Extranet sus respectivas VLANs, también le estoy dando a la red de la Matriz otra característica que es la escalabilidad.

Todo el análisis que se ha citado anteriormente, acerca de que servidores utilizan cada departamento en la red de la Matriz, la asignación de los departamentos a sus respectivas VLANs, la cantidad de equipos que maneja cada departamento y un resumen de la cantidad de hosts por cada VLAN se detalla en la Tabla 3.6

Vale aclarar que las impresoras de red, como es lógico pertenecerán a la VLAN de los usuarios que usan estos equipos. Lo cual ayuda a que los pedidos de multicast o broadcast para imprimir solo se propaguen dentro de su propia VLAN y no afecte al resto, además que no existirá ningún tipo de enrutamiento lo cual beneficia en la latencia de los paquetes.

ASIGNACIÓN DE VLAN's EN LA MATRIZ - PETROCOMERCIAL

Equipos			Cantidad de clientes x VLAN								VLAN's								AS/400's				SERVIDORES					DEPARTAMENTOS	ID
# PC	# IMP	# EQ	GEST.RED	GEST.SERV	VOZ	ADMIN	COMERC	GENERAL	FILIALES	INTERNET	GEST.RED	GEST.SERV	VOZ	ADMIN	COMERC	GENERAL	FILIALES	INTERNET	PCO1	PCO2	PCO8	PCO9	PCORED	PCORED1	PCORED4	PCORED5	PCORED7		
5						5								4					X	X	X		X	X				**CONTRALORIA GENERAL DEL ESTADO**	CTR
1						1								4					X				X	X				**CAJITA DE PCO**	CPECO
6						6								4					X	X			X	X				**FONDO DE JUBILACION**	
9								9								6					X			X	X			&	**VICEPRESIDENCIA (Asesores de Vicepresidencia)**	VCP
3								3								6								X	X			&	LEGAL VICEPRESIDENCIA (Asesoria Legal)	VLE
5						5								4					X	X	X			X	X			&	PLANIFICACION Y FINANZAS	VPF
6							6								5						X			X	X	X		&	PROGRAMACION	VPR
2								2								6								X	X			&	RELACIONES PUBLICAS	VRP
7								7								6				X				X	X	X		&	CONTROL DE GESTION	VCG
5								5								6								X	X			&	**GERENCIA REGIONAL NORTE**	VGN
8	1					9								4					X					X	X			&	**COORDINACION DE CONTRATOS**	GCC
2						2								4					X	X				X	X			&	**CONTROL DE GESTION**	GCG
12	1							13								6								X	X			&	**LEGAL GERENCIA NORTE**	GLE
0								0								6								X	X			&	ASESORIAS	LAS
4								4								6								X	X				PROCESOS	LPR
3						3								4						X				X	X	X		&	**PROYECTOS**	GPR
7								7								6								X	X			&	EJECUCION DE PROYECTOS	PEP
4								4								6								X	X				EVALUACION DE PROYECTOS	PEV
0								0								6								X	X				REAJUSTE DE PRECIOS	PRP
4	4			8								2							X	X	X	X	X	X	X	X	X	&	**SISTEMAS Y TELECOMUNICACIONES**	GSI
6		15		6								2							X	X	X	X	X	X	X	X		&	INGENIERIA Y PROCESAMIENTO	SIP
4		7	4								1												X	X					REDES Y TELECOMUNICACIONES	SRT
19	1			20								2							X	X	X	X	X	X	X			&	SOPORTE Y APLICACIONES	SSA
7	1			8								2							X	X	X	X	X	X	X	X		&	SOPORTE TECNICO Y MANTENIMIENTO	SST
2								2								6							X	X				&	**SUBGERENCIA DE ADMINISTRACION Y FINANZAS**	GSA
3						3								4					X	X			X	X				&	**ADMINISTRATIVA**	AAD
2						2								4					X				X	X				&	BIENESTAR LABORAL	DBL
8						8								4					X	X			X	X	X			&	RECURSOS HUMANOS	DRH
11	1					12								4					X		X		X	X				&	SERVICIOS ADMINISTRATIVOS	DSA
3		1						4								6							X	X				&	SEGURIDAD FISICA	DSF
4								4								6							X	X				&	SECRETARIA GENERAL	DSG
2						2								4					X	X	X		X	X				&	**FINANZAS**	AFI
5						5								4					X	X			X	X				&	ADMINISTRACION DE ACTIVOS	FAA
10						10								4					X	X			X	X				&	ADMINISTRACION FINANCIERA	FAF
9							9								5					X	X		X	X				&	CREDITO Y COBRANZAS	FCC
15	1					16								4					X	X	X		X	X				&	CONTABILIDAD	FCO
4	1					5								4					X	X	X		X	X				&	PRESUPUESTO	FPR
6						6								4					X		X		X	X				&	SEGUROS Y GARANTIAS	FSG
4						4								4					X	X			X	X				&	CUENTAS POR PAGAR	FCP
2						2								4					X	X			X	X	X			&	**MATERIALES**	AMA
5						5								4					X				X	X					COMPRAS LOCALES	MCL
5						5								4					X				X	X					IMPORTACIONES	MIM
5						5								4					X				X	X					CONTROL DE MATERIALES Y BODEGAS	MCM
2							2								5						X		X	X	X			&	**SUBGERENCIA DE COMERCIALIZACION**	GSC
2	2						4								5						X		X	X	X			&	**ABASTECEDORA**	CAB
6							6								5					X	X		X	X				&	FACTURAS Y VENTAS	BFV
4							4								5						X		X	X				&	LIQUIDACION Y CONSOLIDACION DE CUENTAS	BLC
5							5								5					X	X		X	X					COORDINACION OPERATIVA	BCO
6	1						7								5						X		X	X	X			&	**COMERCIALIZADORA**	CKO
2							2								5					X	X		X	X				&	ADMINISTRACION DE NEGOCIOS PROPIOS	KAN
3							3								5					X	X		X	X	X				COORDINACION OPERATIVA DE VENTAS	KCO
3							3								5					X	X		X	X				&	MERCADEO Y ATENCION AL CLIENTE	KMA
8	1						9								5						X		X	X				&	**SUBGERENCIA DE TRANSPORTE Y ALMACENAMIENTO**	GST
																					X		X	X				&	**MOPRO**	TMP
				3		4	2					2		4	5														SERVIDORES o AS400's	
				1								2																	FIREWALL	
			6								1																		ROUTERS	
			14								1																		SWITCHES (DEL NUEVO DISEÑO)	
					139								3																TELEFONOS IP Y CENTRAL	
									1								7												FILIALES	
										6								8											EXTRANET (INTERNET) y SERVIDOR WEB	
												2		4	5	6													IMPRESORAS DE RED (De acuerdo al departamento)	
			24	46	139	125	62	64	1	6																				

24	GESTION DE RED	VLAN1
46	GESTION DE SERVIDORES	VLAN2
139	VOZ	VLAN3
125	ADMINISTRATIVA	VLAN4
62	COMERCIALIZACION	VLAN5
64	GENERAL	VLAN6
1	FILIALES	VLAN7
6	EXTRANET	VLAN8

& Solo las Secretarias de las Unidades utilizan el Sistema Documental de PCORED7

Tabla 3.6 Análisis para la Asignación de VLANs

3.1.7.3 Departamentos asignados a VLANs

VLAN 1 - GESTION DE RED

Telecomunicaciones

Swtiches Cisco

VLAN 2 – GESTION DE SERVIDORES

Ingeniería y Procesamiento

Redes y Telecomunicaciones

Soporte y Aplicaciones

Soporte Técnico y Mantenimiento

Servidores Empresariales: PCORED, PCORED1 y PECORED 7

Computadoras con direcciones controladas por el Firewall

Impresoras de la Unidad de Sistemas y Telecomunicaciones

VLAN 3 - VOZ

Controlador de la Central IP Mitel

E2T de la Central IP Mitel

Teléfonos IP Mitel

VLAN 4 - ADMINISTRATIVA

Contraloría General del Estado

Cajita de PCO

Fondo de Jubilación

Planificación y Finanzas

Coordinación de Contratos

Control de Gestión (Gerencia)

Proyectos

Administrativa

Bienestar Laboral

Recursos Humanos

Servicios Administrativos

Finanzas

Administración de Activos
Administración Financiera
Contabilidad
Presupuesto
Seguros y Garantías
Cuentas por Pagar
Materiales
Compras Locales
Importaciones
Control de Materiales y Bodegas

Impresoras de Presupuesto, Servicios Administrativos, Contabilidad y Coordinación de Contratos
Servidores de grupo de trabajo: PCO1, PCO2, PECORED 4 y PCORED 5.

VLAN 5 - COMERCIALIZACION
Programación
Crédito y Cobranzas
Subgerencia de Comercialización
Abastecedora
Facturas y Ventas
Liquidación y consolidación de Cuentas
Coordinación Operativa
Comercializadora
Administración de Negocios Propios
Coordinación Operativa de Ventas
Mercadeo y Atención al Cliente.
Subgerencia de Transporte y Almacenamiento

Impresoras de Abastecedora, Comercializadora y Subgerencia de Transporte
Servidores de grupo de trabajo: PCO8 y PCO9.

VLAN 6 - GENERAL
Vicepresidencia

Legal Vicepresidencia

Relaciones Públicas

Control de Gestión (Vicepresidencia)

Gerencia Regional Norte

Legal Gerencia Norte

Asesorías

Procesos

Ejecución de proyectos

Evaluación de proyectos

Reajuste de precios

Subgerencia de Administración y Finanzas

Seguridad Física

Secretaría General

Impresora de Legal Gerencia Norte

VLAN 7 – FILIALES

Router Cisco 3600 (Petroecuador, Petroproducción, Oleoducto)

VLAN 8 - EXTRANET

Router IBM 2210 (Internet, SRI, DNH)

Servidor Web

3.1.7.4 Nuevo Direccionamiento IP para la Red de la Matriz

Cada VLAN debe pertenecer a una subred diferente, lo cual indica que debemos sub-netear la red que le han asignado a la red de la Matriz, que es 172.20.64.0/21.

De acuerdo a la propuesta realizada, cada conexión con los routers y la conexión con el Firewall, deben estar en subredes diferentes, por lo tanto se designo que la subred 172.20.64.0/25, es decir el rango desde la dirección 172.20.64.1 a la 172.20.64.126, se utilicen para crear subredes de cada uno de los accesos mencionados. Ver Tabla 3.7.

Para la creación del nuevo direccionamiento IP de las VLANs se tomo en consideración la cantidad de usuarios que pertenecen a cada una de ellas y el dejar un rango mínimo del 100% para el crecimiento de estas.

Como se muestra en la Tabla 3.7, en el nuevo direccionamiento, la VLAN de Comercialización y la VLAN General podrían estar sin problema en las sub-redes 172.20.67.0/25 y 172.20.67.128/25, pero como ventajosamente no tenemos restricción o necesidad de ahorrar direcciones porque tenemos todavía muchas direcciones disponibles, se decidió por ubicarles en las sub-redes 172.20.67.0/24 y 172.20.68.0/24, especialmente porque ayudarán al administrador a ubicarse fácilmente en la VLAN respectiva sólo con ver la dirección IP.

Como ya se mencionó anteriormente, es necesario recalcar que esta nueva propuesta de diseño de VLANs implica un cambio radical de las direcciones de todos los hosts de la red, incluyendo a Servidores, Firewall e interfaces LAN de los routers, por lo cual esta actividad se debe realizar con mucha precaución, realizando planes estratégicos para migrar de una dirección a otra, y tratar de afectar en lo menos posible el desempeño de las actividades de los usuarios y de la empresa en general. Para realizar estos cambios de direcciones utilizar la Tabla 3.7 y la Tabla 3.8.

NUEVO DIRECCIONAMIENTO IP DE LA MATRIZ PROPUESTA 2				
172.20.64.0/21	172.20.64.0/30	172.20.64.0 172.20.64.1 172.20.64.2 172.20.64.3	Acceso al Router Vanguard Motorola (Frame Relay)	Accesos a Routers 64.1 - 64.126
	172.20.64.4/30	172.20.64.4 172.20.64.5 172.20.64.6 172.20.64.7	Acceso al Firewall IBM AIX (Filiales y Extranet)	
	172.20.64.8/30	172.20.64.8 172.20.6.9 172.20.64.10 172.20.64.11	Acceso al Router Cisco 800 Series (Sucursales:Gyql, Cuenca, Riobamba)	
	172.20.64.12/30	172.20.64.12 172.20.64.13 172.20.64.14 172.20.64.15	Acceso al Router IBM 2216-400 (Terminales: Corazón, Chalpi)	
	172.20.64.16/30	172.20.64.16 172.20.64.17 172.20.64.18 172.20.64.19	Acceso al Router IBM 2210 (Acceso Dial-Up)	
		...	Direcciones Libres	
	172.20.64.128/25	172.20.64.128		VLAN 1
		172.20.64.129	Switch Cisco 4507R y **Gateway para la VLAN 1**	
		172.20.64.130 ... 172.20.64.169	Switches Cisco	
		172.20.64.170 ... 172.20.64.199	Scope del DHCP para las PC's de la VLAN de Gestión de Red	
		172.20.64.200 ... 172.20.64.209	Impresoras para la VLAN DE GESTION DE RED	
			Direcciones Libres	
		172.20.64.255		
	172.20.65.0/24	172.20.65.0		VLAN 2
		172.20.65.1	**Gateway para la VLAN 2**	
		172.20.65.2 ... 172.20.65.49	Direcciones para control del Firewall	
		172.20.65.50 ... 172.20.65.69	Servidores Empresariales	
		172.20.65.70 ... 172.20.65.229	Scope del DHCP para las PC's de la VLAN de Gestion de Servidores	
		172.20.65.230 ... 172.20.65.254	Impresoras para la VLAN DE GESTION DE SERVIDORES	
		172.20.65.255		
	172.20.66.0/24	172.20.66.0		VLAN 3
		172.20.66.1	**Gateway para la VLAN 3**	
		172.20.66.2	Dirección Estática (Central Telf. IP)	
		172.20.66.3	Dirección estática del E2T (Central)	
		172.20.66.10 ... 172.20.66.220	Direcciones asignadas al DHCP de la Cental IP Mitel para los teléfonos IP	
		... 172.20.66.255		
	172.20.67.0/24	172.20.67.0		VLAN 4
		172.20.67.1	**Gateway para la VLAN 4**	
		172.20.67.2 ... 172.20.67.10	Servidores y AS400's	
		172.20.67.11 ... 172.20.67.229	Scope del DHCP para las PC's de la VLAN Administrativa	
		172.20.67.230 ... 172.20.67.254	Impresoras para la VLAN ADMINISTRATIVA	
		172.20.67.255		
	172.20.68.0/24	172.20.68.0		VLAN 5
		172.20.68.1	**Gateway para la VLAN 5**	
		172.20.68.2 ... 172.20.68.10	Servidores y AS400's	
		172.20.68.11 ... 172.20.68.229	Scope del DHCP para las PC's de la VLAN de Comercialización	
		172.20.68.230 ... 172.20.68.254	Impresoras para la VLAN COMERCIALIZACION	
		172.20.68.255		
	172.20.69.0/24	172.20.69.0		VLAN 6
		172.20.69.1	**Gateway para la VLAN 6**	
		172.20.69.2 ... 172.20.69.229	Scope del DHCP para las PC's de la VLAN General	
		172.20.69.230 ... 172.20.69.254	Impresoras para la VLAN GENERAL	
		172.20.69.255		
		172.20.70.0 ... 172.20.70.255 172.20.71.0 ... 172.20.71.255	Direcciones Libres	
	10.10.10.0/24	10.10.10.17	Filiales	VLAN 7
	200.24.212.16/29	200.24.212.17 ... 200.24.212.22	Extranet (Internet)	VLAN 8

Tabla 3.7 Nuevo Direccionamiento IP para la Red de la Matriz

A continuación se muestra en la Tabla 3.8 el detalle de la asignación de direcciones IP a los respectivos equipos de acuerdo a las sub-redes creadas para cada VLAN.

Detalle de Direcciones IP de la Matriz - Quito			
PROPUESTA 2			
Rango	Detalle	Descripción	VLAN
64.1 - 64.126 Comunicaciones	.1	Router Vanguard Motorola	
	.2	Interfaz del Switch Multilayer al Router Vanguard	
	.5	Firewall IBM AIX (Interna)	
	.6	Interfaz del Switch Multilayer al Firewall IBM AIX	
	.9	Router CISCO 800 Series	
	.10	Interfaz del Switch Multilayer al Router Cisco 800 Series	
	.13	Router IBM 2216-400 (Corazón, Chalpi)	
	.14	Interfaz del Switch Multilayer al Router IBM 2216-400	
	.17	Router IBM 2210 Dial up	
	.18	Interfaz del Switch Multilayer al Router IBM 2210	
	.15 - .126	Libres	
64.129	.129	Switch Multilayer Cisco 4507R y Gateway para la VLAN 1	VLAN1
64.130 - 64.169 Switches Cisco	.130	Switch Cisco Pco_66	
	.131	Switch Cisco Pco_67	
	.132	Switch Cisco Pco_68	
	.133	Switch Cisco Pco_69	
	.134	Switch Cisco Pco_70	
	.135	Switch Cisco Pco_71	
	.136	Switch Cisco Pco_72	
	.137	Switch Cisco Pco_73	
	.138	Switch Cisco Pco_74	
	.139	Switch Cisco Pco_75	
	.140	Switch Cisco Pco_76	
	.141	Switch Cisco Pco_77	
	.142	Switch Cisco Pco_78	
65.170 - 65.199		Scope del DHCP para las PC's de la VLAN de Gestión de Red	
65.200 - 64.209 Impresoras			
.210 - .254		Libres	
65.1	.1	Gateway para la VLAN 2	VLAN2
65.2 - 65.49 Direcciones para control del Firewall	.2 - .29	Libres	
	.30	Libre	
	.31	Soporte de Aplicaciones (SSAFT)	
	.32	Libre	
	.33	Libre	
	.34	Libre	
	.35	Libre	
	.36	Libre	
	.37	Libre	
	.38	Libre	
	.39	Control de Gestión (VCGFE)	
	.40	Libre	
	.41	Seguros y Garantías (FSGMT)	
	.42	Seguros y Garantías (FSGMV)	
	.43	Libre	
	.44	Seguros y Garantías (FSGFG)	
	.45	Contratos de Contratos (GCCXE)	
	.46	Coordinación de Contratos (GCCWG)	
	.47	Coordinación de Contratos (GCCWG)	
	.48	Coordinación de Contratos (GCCWG)	
	.49	Libre	
65.50 - 65.69 Servidores Empresariales	.50	Pcored	
	.51	Pcored1	
	.52	Pcored2	
	.53	Pcored3	
	.54	Libre	
	.55	Libre	
	.56	Pcored6	
	.57	Pcored7	
	.58	Libre	
	.59	Libre	
	.60	Libre	
	.61	Libre	
	.62	Libre	
	.63	Libre	
	.64	Libre	
	.65	Libre	
	.66	Libre	
	.67	Libre	
	.68	Libre	
	.69	Libre	
65.70 - 65.229		Scope del DHCP para las PC's de la VLAN de Gestion de Servidores	
65.230 - 65.254 Impresoras	.236	Impresora Lexmark C720 (Soporte y Aplicaciones) 4to p	
	.238	Impresora IBM Infoprint 1145 (Sistemas) 5to p	
	.239	Impresora IBM Infoprint 1145 (Sistemas) 5to p	
	.240	Impresora Lexmark T522 (Sistemas y Telec.) 5to p	
	.241	Impresora Lexmark C720 (Sistemas y Telec.) 5to p	
	.250	Impresora Lexmark Optra 1650 (Mtto. Sistemas)Ex_pb	
66.1	.1	Gateway para la VLAN 3	VLAN3
66.2	.2	Controlador de la Central IP Mitel	
66.3	.3	E2T de la Central IP Mitel	
66.10 - 66.220		Direcciones del DHCP de la Central para la teléfonos IP	
67.1	.1	Gateway para la VLAN 4	VLAN4
67.2 - 67.10 Servidores y AS400's	.2	Pco1	
	.3	Pco2	
	.4		
	.5		
	.6		
	.7	Pcored4	
	.8	Pcored5	
	.9		
	.10		
67.11 - 67.229		Scope del DHCP para las PC's de la VLAN Administrativa	
67.230 - 67.254 Impresoras	.232	Impresora Lexmark Optra 1650 (Presupuesto)2do p	
	.238	Impresora Lexmark T522 (Servicios Admin.) 5to p	
	.239	Impresora Lexmark T522 (Servicios Admin.) 5to p	
	.244	Impresora Lexmark Optra 1650 (Contabilidad) 8vo p	
	.248	Impresora Lexmark Optra 1650 (Coor. Contratos) Ex_1er p	
68.1	.1	Gateway para la VLAN 5	VLAN5
68.2 - 68.10 Servidores y AS400's	.2	Pco8	
	.3	Pco9	
	.4 - .10		
68.11 - 68.229		Scope del DHCP para las PC's de la VLAN de Comercialización	
68.230 - 68.254 Impresoras	.232	Impresora Lexmark T522 (Abastecedora) 2do p	
	.233	Impresora Lexmark Optra 1650 (Abastecedora) 2do p	
	.234	Impresora Lexmark T522 (Comercializadora) 3er p	
	.243	Impresora HP (Subgerencia de Transporte) 7mo p	
69.1	.1	Gateway para la VLAN 6	VLAN6
69.2 - 69.229		Scope del DHCP para las PC's de la VLAN General	
69.230 - 69.254 Impresoras	.230	Impresora Lexmark T522 (Legal Gerencia Norte) 9no p	
70.1 - 71.254		Direcciones Libres	
10.10.10.17	.17	Firewall IBM AIX (Filiales)	VLAN7
200.24.212.17	.17	Router IBM 2210 (INTERNET, SRI, DNH)	VLAN8
200.24.212.18	.18	NAT de PCO8	
200.24.212.19	.19	Libre	
200.24.212.20	.20	Libre	
200.24.212.21	.21	Pcoweb	
200.24.212.22	.22	Firewall IBM AIX (Externa)	

Tabla 3.8 Detalle de Direcciones IP para la Red de la Matriz

La siguiente tabla resume las VLANs a ser creadas, con su respectiva asignación de direcciones IP.

RESUMEN DEL RANGO DE DIRECCIONES IP PARA CADA VLAN DE LA MATRIZ - PROPUESTA 2						
VLAN #	**Nombre**	**Rango Util de direcciones**	**Máscara**	**/#**	**Nro. De Clientes**	**Común acceso a:**
	Accesos a Routers y Firewall	172.20.64.1 - 172.20.64.126	255.255.255.252	/30	2/acceso	
VLAN 1	Vlan de Gestion de Red	172.20.64.129 - 172.20.64.254	255.255.255.128	/25	24	
VLAN 2	Vlan de Gestion de Servidores	172.20.65.1 - 172.20.65.254	255.255.255.0	/24	46	
VLAN 3	Vlan de Voz	172.20.66.1 - 172.20.66.254	255.255.255.0	/24	139	
VLAN 4	Vlan Administrativa	172.20.67.1 - 172.20.67.254	255.255.255.0	/24	125	PCO1,PCO2, PCORED4, PCORED5
VLAN 5	Vlan de Comercialización	172.20.68.1 - 172.20.68.254	255.255.255.0	/24	62	PCO8, PCO9
VLAN 6	Vlan General	172.20.69.1 - 172.20.69.254	255.255.255.0	/24	64	PCORED, PCORED1, PCORED7
VLAN 7	Vlan de Filiales	10.10.10.17			1	
VLAN 8	Vlan de la Extranet (Internet)	200.24.212.17 - 200.24.212.22	255.255.255.248	/29	6	

Tabla 3.9 Resumen de VLANs para la Red de la Matriz

En la siguiente tabla se muestra la asignación de VLANs por cada cluster del nuevo diseño propuesto:

Piso	Departamento	Us/Rack	VLAN1	VLAN2	VLAN3	VLAN4	VLAN5	VLAN6	
9no	Legal Gerencia Norte (1 impresora+1 telf ind)	73			3			6	CLUSTER 1
	Seguridad Física (1 equipo)				3			6	
8vo	Subgerencia de Administración y Finanzas				3			6	
	Recursos Humanos				3	4			
	Servicios Administrativos (1 impresora + 1 telf ind)				3	4			
7mo	Administrativa				3	4			
	Materiales				3	4			
	Subgerencia de Transporte y Almacenamiento (1 imp.+ 2 telf ind)				3		5		
6to	Vicepresidencia (3 telf ind)	98			3			6	
5to	Ingeniería y Procesamiento (15 ptos para equipos)			2	3				
	Redes y Telecomunicaciones (7 ptos equipos + 2Telf ind)		1		3				
	Sistemas y Telecomunicaciones (4 impresoras + 2 telf ind)			2	3				
	Soporte Técnico y Mantenimiento (1 impresora)			2	3				
4to	Soporte de aplicaciones			2	3				
	Legal Vicepresidencia				3			6	
	Planificación y Finanzas				3	4			
	Programación				3		5		
3er	Subgerencia de Comercialización	82			3		5	6	CLUSTER 2
	Gerencia Regional Norte				3				
	Comercializadora (1 impresora)				3		5		
2do	Abastecedora (con 2 impresoras)				3		5		
	Finanzas (1 telf ind)				3	4			
	Presupuesto (1 impresora + 1 telf ind)				3	4			
1er	Administración de Negocios Propios				3		5		
	Crédito y Cobranzas (1 telf. ind.)				3		5		
	Seguros y Garantías				3	4			
	Contabilidad (1 impresora)				3	4			
PB	Secretaría General (1 telf ind)	30			3			6	CLUSTER 3
	Administración de Activos				3	4			
	Administración Financiera (2 telf. Ind.)				3	4			
	Cuentas por Pagar				3	4			
	Servicios Administrativos (Recepción Rocio)				3	4			
Sub	Servicios Administrativos (Mtto. Eléctrico)					4			
	Cajita de PCO					4			

2do	Relaciones Públicas (1 telf ind)	28			3			6	CLUSTER 4
	Control de Gestión (VCP) (3 telf ind)				3			6	
	Control de Gestión (VGN)				3	4			
1er	Bienestar Laboral (2 telf ind.)				3	4			
	Coordinación de Contratos (1 impresora)				3	4			
	Proyectos (1 telf ind)	27			3	4			
PB	Fondo de Jubilación Especial					4			
	Proyectos				3	4			
	Soporte Técnico y Mantenimiento (1 impresora)			2					
	Servicios Administrativos-Recepción (1 telf ind)				3	4			

Tabla 3.10 Asignación de VLANs por Ubicación

La Tabla 3.10 permite concluir que es necesario configurar VTP *Pruning* en la red, para que el tráfico de las VLANs solo viaje por los enlaces troncales necesarios y no consuman ancho de banda los paquetes (*flooding)*, cuando viajan hacia clusters o switches en donde no están asignadas éstas VLANs.

El detalle de la asignación de direcciones IP de las impresoras de red de acuerdo a su respectiva VLAN se muestra en la Tabla 3.11.

DIRECCIONES IP DE IMPRESORAS DE RED DE LA MATRIZ - PROPUESTA 2			
65.230 - 65.254 Impresoras	.230	Impresora 1er piso	VLAN2
	.231	Impresora 1er piso	
	.232	Impresora 2do piso	
	.233	Impresora 2do piso	
	.234	Impresora 3er piso	
	.235	Impresora 3er piso	
	.236	Impresora Lexmark C720 (Soporte y Aplicaciones) 4to p	
	.237	Impresora 4to piso	
	.238	Impresora IBM Infoprint 1145 (Sistemas) 5to p	
	.239	Impresora IBM Infoprint 1145 (Sistemas) 5to p	
	.240	Impresora Lexmark T522 (Sistemas y Telec.) 5to p	
	.241	Impresora Lexmark C720 (Sistemas y Telec.) 5to p	
	.242	Impresora 6to piso	
	.243	Impresora 6to piso	
	.244	Impresora 7mo piso	
	.245	Impresora 7mo piso	
	.246	Impresora 8vo piso	
	.247	Impresora 8vo piso	
	.248	Impresora 9no piso	
	.249	Impresora 9no piso	
	.250	Impresora Lexmark Optra 1650 (Mtto. Sistemas)Ex_pb	
	.251	Impresora Ex - salesianos	
66.230 - 66.254 Impresoras	.230	Impresora 1er piso	VLAN4
	.231	Impresora 1er piso	
	.232	Impresora Lexmark Optra 1650 (Presupuesto)2do p	
	.233	Impresora 2do piso	
	.234	Impresora 3er piso	
	.235	Impresora 3er piso	
	.236	Impresora 4to piso	
	.237	Impresora 4to piso	
	.238	Impresora Lexmark T522 (Servicios Admin.) 5to p	
	.239	Impresora Lexmark T522 (Servicios Admin.) 5to p	
	.240	Impresora 6to piso	
	.241	Impresora 6to piso	
	.242	Impresora 7mo piso	
	.243	Impresora 7mo piso	
	.244	Impresora Lexmark Optra 1650 (Contabilidad) 8vo p	
	.245	Impresora 8vo piso	
	.246	Impresora 9no piso	
	.247	Impresora 9no piso	
	.248	Impresora Lexmark Optra 1650 (Coor. Contratos) Ex_1er p	
	.249	Impresora Ex - salesianos	
67.230 - 67.254 Impresoras	.230	Impresora 1er piso	VLAN5
	.231	Impresora 1er piso	
	.232	Impresora Lexmark T522 (Abastecedora) 2do p	
	.233	Impresora Lexmark Optra 1650 (Abastecedora) 2do p	
	.234	Impresora Lexmark T522 (Comercializadora) 3er p	
	.235	Impresora 3er piso	
	.236	Impresora 4to piso	
	.237	Impresora 4to piso	
	.238	Impresora 5to piso	
	.239	Impresora 5to piso	
	.240	Impresora 6to piso	
	.241	Impresora 6to piso	
	.242	Impresora 7mo piso	
	.243	Impresora HP (Subgerencia de Transporte) 7mo p	
	.244	Impresora 8vo piso	
	.245	Impresora 8vo piso	
	.246	Impresora 9no piso	
	.247	Impresora 9no piso	
	.248	Impresora Ex - salesianos	
	.249	Impresora Ex - salesianos	
68.230 - 68.254 Impresoras	.230	Impresora Lexmark T522 (Legal Gerencia Norte) 9no p	VLAN6
	.231	Impresora 1er piso	
	.232	Impresora 2do piso	
	.233	Impresora 2do piso	
	.234	Impresora 3er piso	
	.235	Impresora 3er piso	
	.236	Impresora 4to piso	
	.237	Impresora 4to piso	
	.238	Impresora 5to piso	
	.239	Impresora 5to piso	
	.240	Impresora 6to piso	
	.241	Impresora 6to piso	
	.242	Impresora 7mo piso	
	.243	Impresora 7mo piso	
	.244	Impresora 8vo piso	
	.245	Impresora 8vo piso	
	.246	Impresora 9no piso	
	.247	Impresora 9no piso	
	.248	Impresora Ex - salesianos	
	.249	Impresora Ex - salesianos	

Tabla 3.11 Detalle de Direcciones IP para las impresoras

3.1.8 Elección del Tipo de asignación a VLANs en la red de la Matriz

En primer lugar es necesario hacer referencia a los tipos de asignación que quedan definitivamente descartados en esta elección. El tipo de asignación a VLANs en base a las direcciones de capa 3 queda descartado, debido a que se está utilizando un servidor DHCP que asigna dinámicamente las direcciones IP de los hosts, y no siempre a los mismos hosts les va a asignar la misma dirección IP. La otra opción que se descarta, es la asignación por el tipo de protocolo, puesto que los hosts utilizan un solo protocolo de capa 3, que es IP, y obviamente no tiene sentido aplicarlo.

El tipo de asignación dinámica a VLANs en base a direcciones MAC es una opción factible a implementar, porque el switch Cisco Catalyst 4500 que se va a instalar en la red de la Matriz, puede actuar como servidor de políticas de administración VLANs (VMPS). Por lo tanto los dos tipos de asignación VLAN a considerar en la elección, son: la asignación estática a VLANs en base a puertos y la asignación dinámica a VLANs en base a direcciones MAC.

Las principales desventajas que conlleva la asignación dinámica en base a direcciones MAC específicamente en la red de la Matriz, son: la falta de confiabilidad en la red, debido a que no existe otro servidor VMPS como respaldo, porque siempre existe la posibilidad que el equipo falle por razones no controladas; otra desventaja, es el impacto en el desempeño de la red, debido a la adición de *overheads* (información que no es parte de los datos) que intercambian el cliente y servidor VMPS, para establecer a que VLANs pertenecen cada una de las direcciones MAC o hosts conectados al switch que hace de cliente VMPS, y más aún cuando se tiene un considerable número de usuarios como lo tiene la red de la Matriz (280 computadoras y 140 teléfonos IP). El principal inconveniente, para poner a funcionar este tipo de asignación, es la recopilación de todas las direcciones MAC de los hosts de la red, que al parecer se había resuelto cuando ya se hizo esta recopilación, pero lamentablemente esta base de datos se ha ido desactualizando debido al continuo movimiento de la red, es decir a los cambios e ingresos de máquinas o tarjetas de red, lo que a la vez ratifica que con este tipo de asignación se dificulta la administración, puesto que siempre que ingrese o salga una computadora de la red, la dirección MAC de esta, debe ser inscrita o excluida de la base de datos del servidor VMPS, y esto se complica aún mas, porque por lo general se renuevan de 60 a 100 computadoras anualmente en la red de la Matriz, y obviamente un pequeño error en cualquier dirección MAC, le deja excluida de la red a esa máquina. E implícitamente otro

punto en contra, es la dificultad en resolver los problemas (*troubleshoot*) de la red. Por otro lado, las ventajas que nos ofrece esta asignación dinámica es que no se necesita administración para realizar desplazamientos de usuarios y la notificación de usuarios desconocidos que quieren ingresar a la red.

Si analizamos a estas ventajas que nos ofrece la asignación dinámica de VLANs en base a direcciones MAC, desde otro punto de vista, este libre desplazamiento de usuarios que incluso actualmente se realiza, no ayuda en la administración y resolución de problemas. Mientras que la asignación estática a VLANs en base puertos, si ofrece un control del movimiento de los usuarios, a cambio de realizar una configuración puerto a puerto de las VLANs y de la necesaria administración cada vez que se mueve un usuario de un lugar a otro, pero vale señalar que la configuración y monitoreo de las VLANs con ésta asignación estática es fácil de realizar. E incluso esta asignación estática es conveniente por que por lo general las computadoras en la red de la Matriz, se mantienen conectadas al mismo punto de red.

Son todas estas razones, las ventajas y desventajas de uno y otro lado, que determinaron que el tipo de asignación a VLANs adecuado para la red de la Matriz, con los equipos que se cuenta actualmente, es, la asignación estática de VLANs en base a puertos.

Aunque, si se eligiera la asignación en base a direcciones MAC, la propuesta específica sería asignando dinámicamente las VLANs a las computadoras y a los teléfonos IP, mientras que a los servidores y equipos de red como switches y routers, se los asignaría estáticamente en base a puertos.

3.2 REDISEÑO DE LA RED DE BEATERIO DE PETROCOMERCIAL

Para el rediseño de esta red se aprovechan los switches Cisco 2900XL que salen de la red La Matriz, una vez que se haya cumplido con el diseño propuesto para esa red.; además de un switch Cisco 3550 que no se encuentra activo y de la fibra óptica monomodo que está tendida pero sin utilizarse.

3.2.1 Análisis de la Red Actual de Beaterio

Como se puede observar en la Figura 3.17, la topología actual de la red de Beaterio es Jerárquica, sin redundancia en las conexiones entre los elementos activos de red, es decir sin un buen grado de confiabilidad; utilizando convertidores de UTP a fibra óptica (*transceiver* 100Base-TX a 100Base-FX), lo que indica que no se aprovecha todo el ancho de banda que nos ofrece la fibra óptica y además utilizando un considerable número de switches de bajo desempeño (switches: DLINK y CNET de 6 puertos).

El campus que constituye la red de Beaterio es extenso, razón por la cual ciertos tramos utilizan fibra óptica monomodo; y por lo cual esta red, mas que por un diseño previsto, por necesidad tiene una topología jerárquica.

La mayor cantidad de quejas por parte de los usuarios, acerca del desempeño de la red, basados en sus aplicaciones, son por parte de las áreas de Poliducto Quito – Ambato - Ribamba y Seguridad Industrial, lo cual es lógico, puesto que estas áreas acceden a la red a través de switches DLINK con convertidores de fibra, además de tener el mayor número de saltos hacia la red de área extendida (WAN) y por ende a los servidores ubicados en la red local de la Matriz.

Actualmente se encuentra tendida fibra óptica monomodo desde el área de Telecomunicaciones a la Sucursal - Comercializadora y desde Bodega a Jet - Fuel, pero por la falta de tarjetas de fibra óptica GBIC-LX y la disponibilidad de equipos que soporten estas tarjetas no se ha podido utilizar estos medios. El único tramo sin utilizar *transceivers* y con fibra óptica es la conexión de Telecomunicaciones a Jefatura.

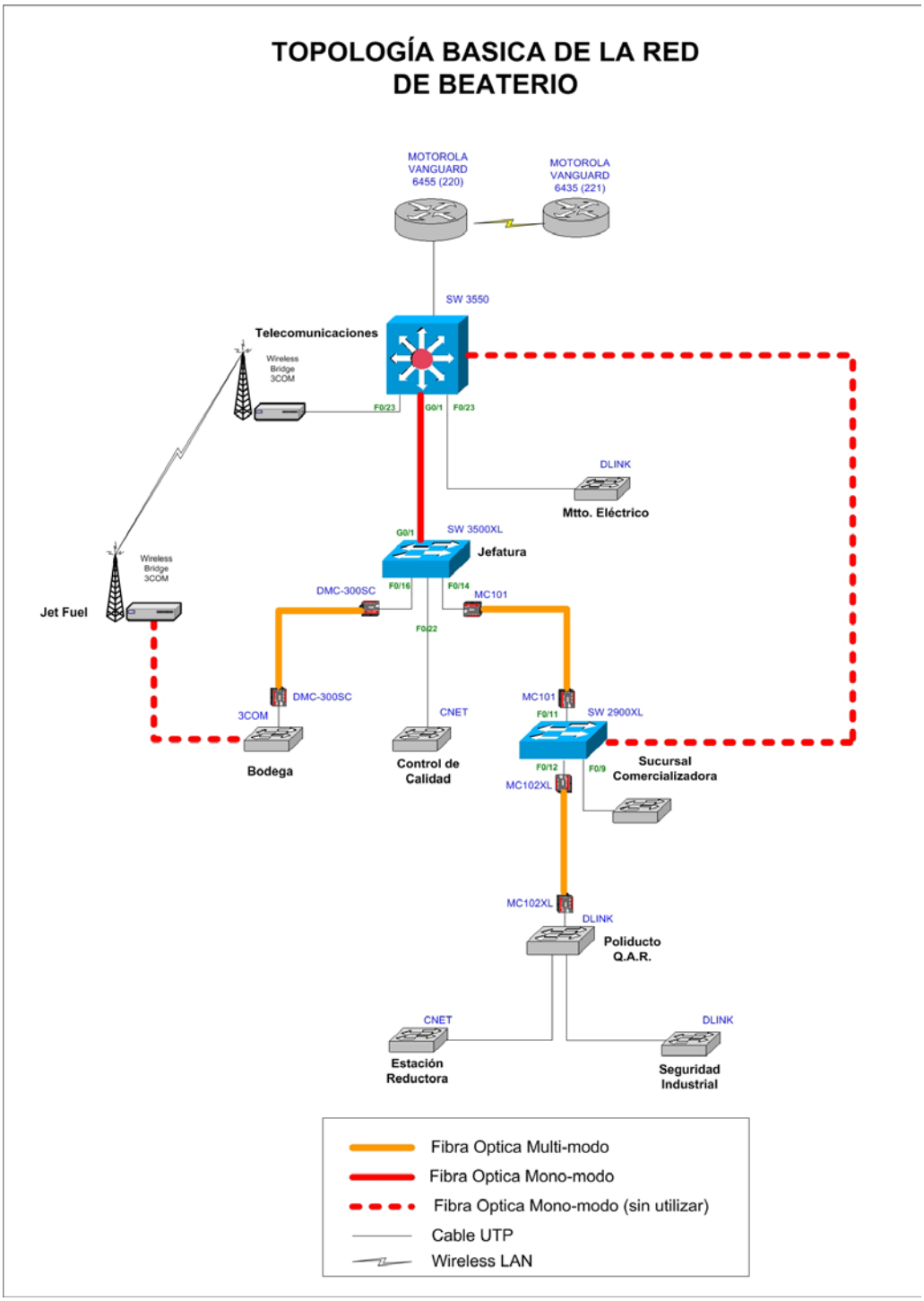


Figura 3.17 Topología Básica de la Red de Beaterio

3.2.2 Disposición de Equipos

Considerando que el backbone de la red de Beaterio va a estar conformada por switches Cisco, en la Tabla 3.12 se detalla la cantidad de estos equipos con los que cuenta actualmente la red.

Cant.	Equipo	Modelo
1	Cisco Catalyst 3550 Series	WS-3550-24-PWR-SMI
1	Cisco Catalyst 3500 XL Series	WS-3524-PWR-XL-EN
1	Cisco Catalyst 2900 XL Series	WS-C2912-XL
3	Tarjetas 1000 Base-LX GBIC	WS-G5486

Tabla 3.12 Equipos Cisco Disponibles en la Red de Beaterio

Los nuevos equipos Cisco disponibles para el mejor desempeño de la red, son:

Cant.	Equipo	Modelo
1	Cisco Catalyst 3550 Series	WS-3550-24-PWR-SMI
1	Cisco Catalyst 2900 XL Series	WS-C2924-XL
1	Cisco Catalyst 2900 XL Series	WS-C2912-XL

Tabla 3.13 Nuevos Equipos Disponibles para la Red de Beaterio

3.2.3 Cableado y Distribución de Usuarios

El cuarto de distribución principal (MDF) se encuentra en el área de Telecomunicaciones, mientras que los cuartos de distribución intermedios (IDF) serán identificados solo a aquellos que posean un armario o rack disponible para la ubicación de equipos de red, como se describe en el siguiente cuadro:

Cuarto	Ubicación de Switches	# Equipos
MDF	TELECOMUNICACIONES	8
IDF1	JEFATURA	8
IDF2	SUCURSAL - COMERCIALIZADORA	8
IDF3	POLIDUCTO Q.A.R	4
IDF4	BODEGA	2
IDF5	JET FUEL	15
	SEGURIDAD INDUSTRIAL	4
	MTTO. ELECTRICO	3
	CONTROL DE CALIDAD	2
	INSPECCION TECNICA	1
	REDUCTORA	1

Tabla 3.14 Cantidad de Equipos por Cuarto de Distribución

Aquellas áreas que no tengan un armario o rack, es porque su cantidad de usuarios es sumamente pequeña, lo cual es una razón más, para solamente utilizar switches pequeños como los: 3COM, CNET o DLINK de seis u ocho puertos.

De acuerdo a la Tabla 3.14, también nos podemos dar cuenta que no será necesario más de un switch por cada cuarto de distribución o área, e incluso con esta consideración se ofrecerá un crecimiento superior al 100%.

Para tener una visualización más clara del tendido de cableado estructurado en la red de Beaterio, a continuación se muestra su respectivo diagrama unifilar:

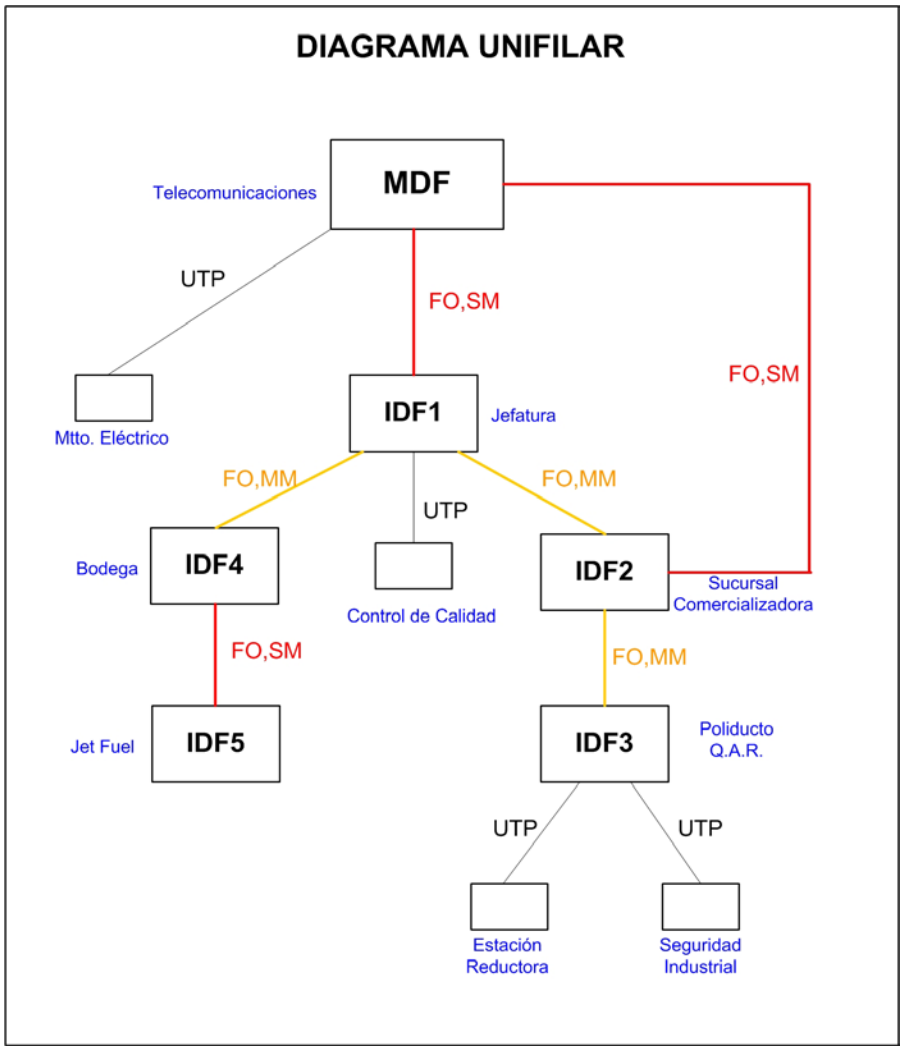


Figura 3.18 Diagrama Unifilar de la Red de Beaterio

Dependiendo del cuarto de distribución se ofrece acceso a varios departamentos independientemente de su localización, como son los siguientes casos:

Telecomunicaciones (MDF):

- Equipos de comunicaciones

- Telecomunicaciones
- Superintendencia de Terminales

Jefatura (IDF 1):

- Jefatura de Mantenimiento. de Terminal
- MOPRO
- Productos Limpios

Sucursal-Comercializadora (IDF 2):

- Sucursal-Comercializadora
- Dispensario Médico

Mantenimiento Electrico:

- Mantenimiento Electrico
- Mantenimiento Industrial

El resto de cuartos de distribución o simplemente los switches, dan acceso solo a sus propios usuarios, en donde se encuentran ubicados.

3.2.4 Consideraciones para el Rediseño de la Red de Beaterio

- Tomar como referencia el modelo jerárquico Cisco, ver en Capítulo 2, Pág. 53.
- Proveer redundancia en el backbone, para dar mayor confiabilidad a la red.
- Aprovechar la fibra óptica monomodo tendida y los nuevos equipos que se tienen a disposición.
- Utilizar las capacidades de capa 3 (del modelo OSI) de los switches Cisco 3550.
- Ubicar los Switches de mejor desempeño en las áreas de mayor tráfico o cantidad de usuarios. Especialmente considerar el proyecto de Automatización y Control de los tanques de almacenamiento de combustible, que se realizará desde Jet- Fuel.
- Además tomar en cuenta la disponibilidad y ubicación de racks en el campus de Beaterio, para colocar los switches Cisco, que necesitan obviamente un lugar adecuado para su instalación.

3.2.5 Red Propuesta para Beaterio

Debido a que el campus de Beaterio es extenso, y además los equipos activos de red son solamente los anteriormente dispuestos, y los medios disponibles de conectividad entre estos equipos son los instalados o tendidos, se presenta una sola propuesta para mejorar la red de Beaterio, como se puede observar en la Figura 3.19.

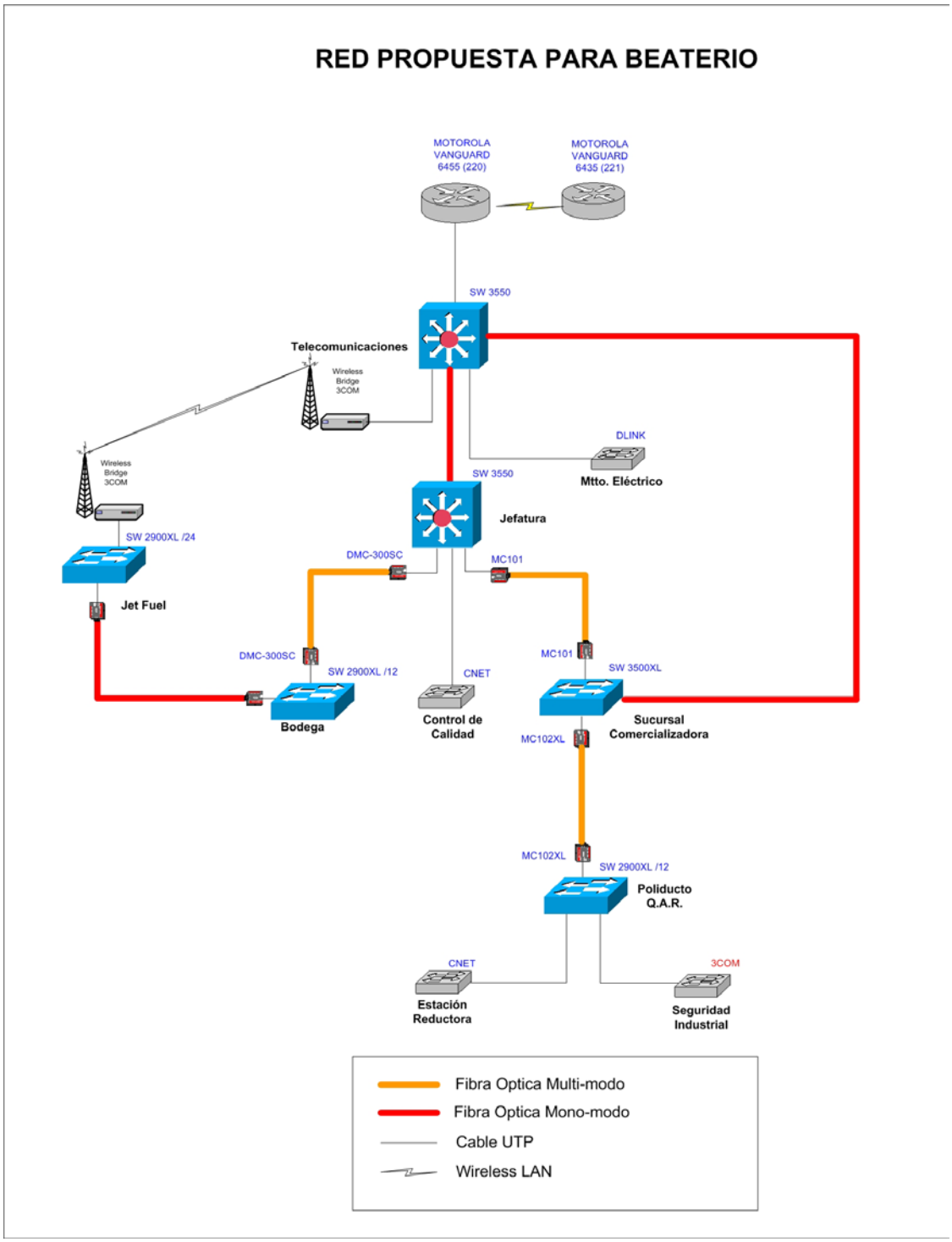


Figura 3.19 Red Propuesta para Beaterio

La nueva alternativa consiste en cerrar un anillo habilitando la fibra monomodo tendida entre Telecomunicaciones y Sucursal – Comercializadora, y además llegar hasta Jet- Fuel con la fibra monomodo desde Bodega. Si se desea tener caminos redundantes para llegar a Jet-Fuel, entonces no se debe deshabilitar el enlace *Wireless* LAN entre éste y Telecomunicaciones, aunque el ancho de banda que ofrece es pequeño. Estos dos nuevos anillos mejoran la confiabilidad y el desempeño de la red.

El nuevo switch Cisco 3550 irá en Jefatura, porque aquí se concentra el tráfico que llega de Jet-Fuel, Bodega, Control de Calidad, y posiblemente de Sucursal-Comercializadora y todo el tráfico debajo de él, si falla la conexión entre éste y Telecomunicaciones. Además que el switch de Jefatura da servicio a departamentos como la Jefatura de Mantenimiento de Terminal, Productos Limpios y MOPRO.

No se consideró habilitar la conexión a 1000 Mbps entre Jefatura y Sucursal – Comercializadora, (es decir la compra de tarjetas 1000Base-SX para los switches de éstas áreas), porque ésta conexión solo será de respaldo en caso de que caigan las conexiones a 1000 Mbps entre Sucursal-Comercializadora y Telecomunicaciones o entre Jefatura y Telecomunicaciones.

El switch Cisco 3500XL de Jefatura pasa a Sucursal-Comercializadora y el switch Cisco 2900XL de doce puertos de ésta área pasa a Poliducto Q.A.R., con la finalidad de ofrecer un mejor servicio tanto a esta última área como a Seguridad Industrial. Aunque no se pueda poner una conexión de 1000 Mbps entre Poliducto Q.A.R. y Sucursal-Comercializadora puesto que el switch Cisco 2900XL no soporta tarjetas GBIC (para fibra óptica), situación que se repite con los switches de Bodega y Jet – Fuel.

Para Jet-Fuel se asigna un switch Cisco 2900XL de 24 puertos, porque se necesitan al menos 15 puertos para los equipos de monitoreo del proyecto de Automatización.

En el futuro, si se adquieren switches que soporten tarjetas GBIC (para fibra óptica) y las propias tarjetas, se podrá mejorar el ancho de banda de las conexiones de 100 Mbps a 1000 Mbps entre las áreas que no lo posean.

Para conseguir el diseño final propuesto se necesita la compra de:

- 2 Tarjetas Cisco 1000 Base-LX, serie: WS-G5486
- 2 *Transceivers* **Allied Telesyn AT-MC102XL** 100Base-TX, 100Base-FX (para fibra mono-modo)

3.2.6 Diseño de VLANs para la Red de Beaterio

Si comparamos las redes propuestas tanto para Beaterio como para la Matriz, podemos decir que son redes similares, simplemente que Beaterio es una red a menor escala, y en lugar de tener varios enlaces a routers de acceso, esta red tiene solamente uno, que es el acceso a la red WAN Frame Relay. Se hace referencia a esto último, porque al igual que en la red de la Matriz, se plantean dos propuestas, las cuales se diferencian solo por el tipo de puerto del switch multilayer (Catalyst 3550 para Beaterio) que se conecta a la interfaz LAN del router.

3.2.6.1 Análisis de Diseños propuestos

La **primera propuesta** (ver Figura 3.20), incluye a la interfaz LAN dentro de la VLAN 1, por lo tanto el switch multilayer utiliza un puerto conmutado (capa 2); mientras que la segunda propuesta le trata a esta conexión como una sub-red mas, es decir el puerto del switch multilayer conectado a esta interfaz es un puerto enrutado con su respectiva dirección IP.

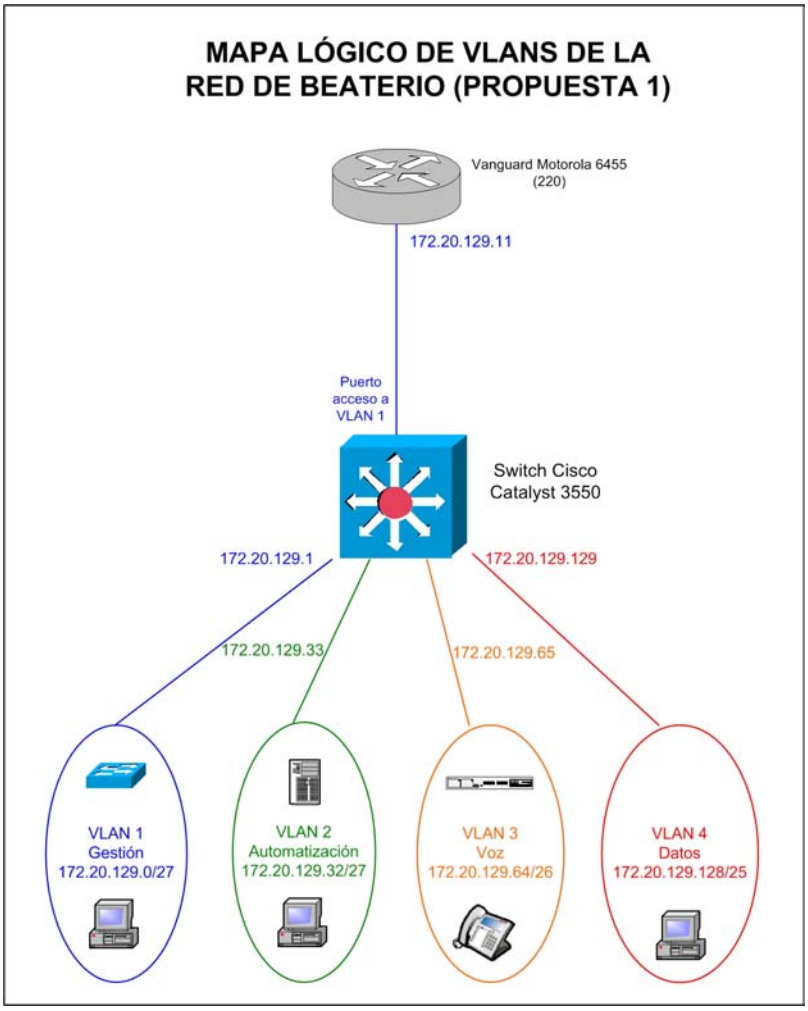


Figura 3.20 Mapa Lógico de VLANs para la Red de Beaterio 1

La **segunda propuesta** (ver Figura 3.21), segmenta adecuadamente el dominio de broadcast de la VLAN 1 al no extenderlo hasta la interfaz del router e interferir con el tráfico que se dirige hacia la WAN, que como es lógico, esto es lo que comúnmente sucede, porque los hosts necesitan comunicarse con los servidores que se encuentran en la red local de la Matriz; y además se ofrece la posibilidad de agregar seguridad en el switch multilayer, en caso de que sea necesario, y especialmente cuando se requiera hacia una VLAN en particular; mientras que la primera propuesta no realiza esto y por ende no tiene estos beneficios.

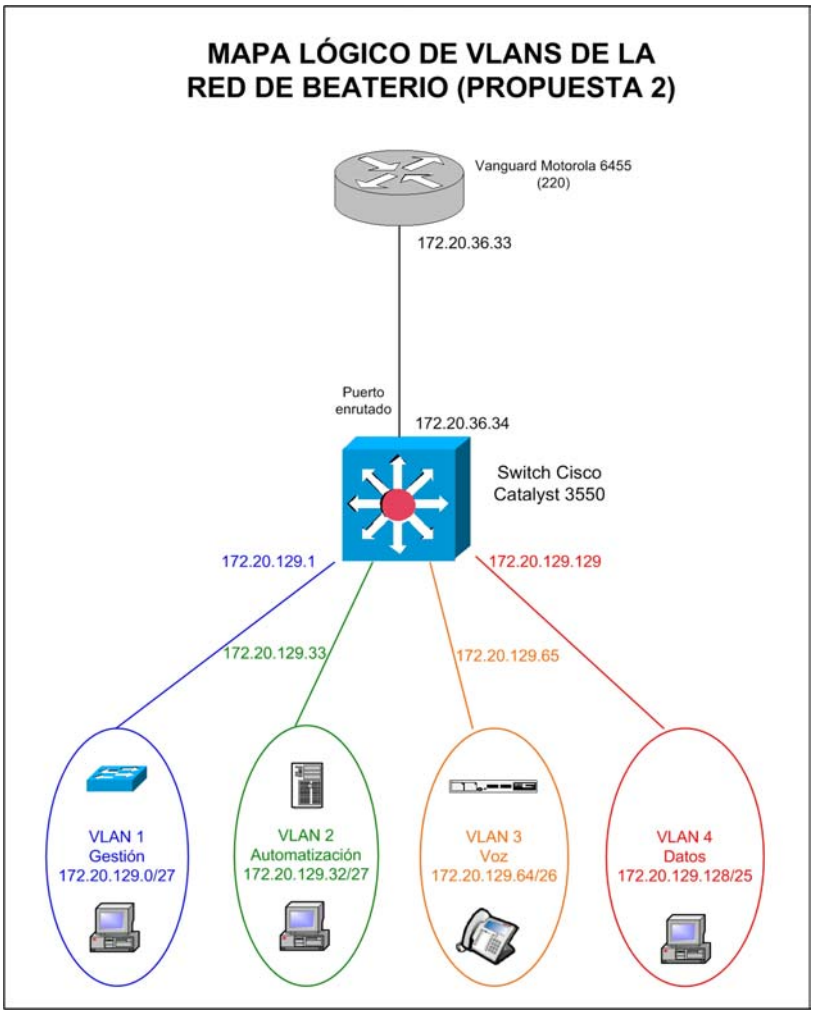


Figura 3.21 Mapa Lógico de VLANs para la red de Beaterio 2

La justificación para implementar la primera propuesta, es que el dominio de broadcast de la VLAN 1 es pequeño y por ende no influye demasiado en el desempeño de la red y además no es muy lógico poner seguridad hacia la WAN Frame Relay porque es parte de la red de Petrocomercial. Por estas razones se incluye toda la información de la primera propuesta de diseño de VLANs en el Anexo 11, en el caso de que la empresa se incline por éste diseño. Pero el presente proyecto elige como mejor propuesta al segundo diseño y por tal razón se expone su análisis a continuación.

3.2.6.2 Desarrollo del Mejor Diseño Propuesto

Al igual que para el diseño de VLANs de la Matriz, para la red de Beaterio también se analizó que servidores utilizan los departamentos, como se muestra en el siguiente cuadro:

ASIGNACIÓN DE VLAN's EN BEATERIO - PETROCOMERCIAL

Cant. Equipos			# Clientes x VLAN			VLAN's			AS/400's				SERVIDORES							DEPARTAMENTOS	ID
# PC	# TEL	# EQ	GESTION	VOZ	DATOS	GESTION	VOZ	DATOS	PCO1	PCO2	PCO8	PCO9	PCORED	PCORED1	PCORED2	PCORED4	PCORED5	PCORED7	PCOWEB		
								3					X	X				&		**PROTECCION AMBIENTAL Y SEGURIDAD INDUSTRIAL**	GPI
1					1			3					X	X						PROTECCION AMBIENTAL	IPA
3					3			3					X	X						SEGURIDAD INDUSTRIAL	ISI
3		2	5			1							X	X						REDES Y TELECOMUNICACIONES	SRT
2					2			3					X	X						BIENESTAR LABORAL (DISPENSARIO MEDICO)	DBL
2					2			3	X				X	X						BODEGA DE BEATERIO	MBB
6					6			3		X	X		X	X				&		SUCURSAL QUITO	BSQ
								3					X	X						**INSPECCION TECNICA**	TIT
								3					X	X						**CONTROL DE CALIDAD**	TCC
1					1			3					X	X						ESTACION REDUCTORA BEATERIO	EEB
2					2			3			X		X	X				&		**SUPERINTENDENCIA POLIDUCTO QUITO-AMBATO-RIOBAMBA**	TPQ
								3					X	X						MANTENIMIENTO ELECTROMECANICO QUITO-AMBATO-RIOBAMBA	QME
1					1			3					X	X						MANTENIMIENTO DE LINEA QUITO-AMBATO-RIOBAMBA	QML
1					1			3					X	X						OPERACIONES QUITO-AMBATO-RIOBAMBA	QOP
								3					X	X						INSPECCION TECNICA POL. QUITO-AMBATO-RIOBAMBA	QIT
2					2			3	X		X		X	X		X		&		**SUPERINTENDENCIA TERMINALES Y DEPOSITOS**	TYD
4					4			3					X	X				&		TERMINALES Y DEPOSITOS	YTD
2					2			3					X	X						CONTROL DE CALIDAD TERMINALES Y DEPOSITOS	YCC
								3					X	X						DESPACHO DE TERMINALES Y DEPOSITOS	YDE
1					1			3					X	X						INSPECCION TECNICA TERMINALES Y DEPOSITOS	YIT
2					2			3			X		X	X						MOPRO TERMINALES Y DEPOSITOS	YMP
4					4			3					X	X				&		MANTENIMIENTO TERMINALES Y DEPOSITOS	YMT
2					2			3			X		X	X				&		TERMINAL PRODUCTOS LIMPIOS BEATERIO	YTB
39																					
			2			1														ROUTERS	
			5			1														SWITCHES (DEL NUEVO DISEÑO)	
				20			2													TELEFONOS IP Y CENTRAL	
			12	20	36																

12 GESTION DE RED Y SERVIDORES
20 VOZ
36 DATOS

& Solo las Secretarias de las Unidades utilizan el Sistema Documental de PCORED7

Tabla 3.15 Análisis para la Asignación de VLANs en Beaterio

Pero realmente si razonamos de acuerdo a la red con la que estamos ahora trabajando, esta información no es de mucha ayuda, porque que todas las VLANs que se pretendería crear igual van a tener que cruzar la red de área extendida (WAN) para acceder a los servidores empresariales ubicados en la red de La Matriz. Es decir las VLANs que se vayan a crear en Beaterio son VLANs geográficas, porque el 80% del tráfico de cada una de las VLANs viajará fuera de su VLAN local, mientras que el 20% del tráfico, se mantendrá dentro de la VLAN.

Además no se puede pretender crear muchas VLANs puesto que la cantidad de usuarios es bastante pequeña. Por lo tanto se decidió crear VLANs de acuerdo a las aplicaciones y tipos de tráfico (voz sobre IP, datos), como se muestra a continuación:

VLAN DE GESTION: Para los switches, y las estaciones de trabajo que administren estos equipos (Telecomunicaciones).

VLAN DE AUTOMATIZACIÓN: Empleada para los equipos involucrados en el proyecto de Automatización y Control.

VLAN DE VOZ: Para los teléfonos IP y Central Telefónica IP Mitel.

VLAN DE DATOS: Para todas las computadoras de todos los departamentos de Beaterio, excepto Telecomunicaciones y las computadoras del proyecto de Automatización y Control.

3.2.6.3 Nuevo Direccionamiento IP para la Red de Beaterio

Tomando en cuenta la cantidad de equipos que existirá por cada VLAN, se estableció el siguiente direccionamiento:

NUEVO DIRECCIONAMIENTO IP DEL BEATERIO (172.20.129.0/24) PROPUESTA 2				
	172.20.36.32/30	172.20.36.32		Acceso a Routers
		172.20.36.33 172.20.36.34	Acceso al Router Vanguard Motorola - 220 (Frame Relay)	
		172.20.36.35		
	172.20.36.32/30	172.20.36.36		
		172.20.36.37 172.20.36.38	Acceso al Router Vanguard Motorola - 221	
		172.20.36.39		
172.20.129.0/24	172.20.129.0/27	172.20.129.0		VLAN 1
		172.20.129.1 ... 172.20.129.10	Switches y **Gateway para VLAN 1 (172.20.129.1)**	
		172.20.129.11 ... 172.20.129.30	Direcciones para las PC's de la **VLAN de GESTION** usando el DHCP de la Central Mitel	
		172.20.129.31		
	172.20.129.32/27	172.20.129.32		VLAN 2
		172.20.129.33	**Gateway para VLAN 2**	
		172.20.129.34 ... 172.20.129.62	Proyecto de Automatización y Control (**VLAN de AUTOMATIZACION**)	
		172.20.129.63		
	172.20.129.64/26	172.20.129.64		VLAN 3
		172.20.129.65	**Gateway para VLAN 3**	
		...		
		172.20.129.68	Dir.estática de una PC para upgrade de software de la Central	
		172.20.129.69	Dirección estática del E2T (Central)	
		172.20.129.70	Dirección estática de la Central Telf. IP MITEL	
		172.20.129.71 ... 172.20.129.100	Direcciones del DHCP de la Central para los teléfonos IP (**VLAN de VOZ**)	
		...		
		172.20.129.127		
	172.20.129.128/25	172.20.129.128		VLAN 4
		172.20.129.129	**Gateway para VLAN 4**	
		172.20.129.130 ... 172.20.129.254	Direcciones para las PC's de la **VLAN de DATOS** usando el DHCP de la Central Mitel	
		172.20.129.255		

Tabla 3.16 Nuevo Direccionamiento IP de Beaterio

En mayor detalle se muestran las direcciones estáticas de los equipos de Beaterio, en la siguiente tabla:

Detalle de Nuevas Direcciones IP de Beaterio - Quito Red: 172.20.129.0/24 - PROPUESTA 2			
Rango	**Detalle**	**Descripción**	VLAN#
Accesos a Routers	172.20.36.33	Router Motorola Vanguard 6455 (220)	
	172.20.36.34	Interfaz del Switch Multilayer al Router 6455	
	172.20.36.37	Router Motorola Vanguard 6435 (221)	
	172.20.36.38	Interfaz del Switch Multilayer al Router 6435	
129.1 - 129.10 Switches	172.20.129.1	Switch Cisco Catalyst 3550 Series y **Gateway para la VLAN 1**	VLAN1
	172.20.129.2	Switch Cisco Catalyst 3500 XL Series	
	172.20.129.3	Switch Cisco Catalyst 2900 XL Series	
	.4 - .10	Libres	
129.11 - 129.30		Direcciones para las PC's de la **VLAN de GESTION** usando el DHCP de la Central Mitel	
.129.33	172.20.129.33	**Gateway para VLAN 2**	VLAN2
129.34 - .129.62		Proyecto de Automatización y Control (**VLAN de AUTOMATIZACION**)	
129.65	172.20.129.65	**Gateway para VLAN 3**	VLAN3
.66 - .67		Libres	
129.68	172.20.129.68	PC para upgrade de software de la Central	
129.69	172.20.129.69	E2T de la Central IP Mitel	
129.70	172.20.129.70	Controlador de la Central IP Mitel	
129.71 - 129.100		Direcciones del DHCP de la Central para los teléfonos IP (**VLAN De VOZ**)	
129.100 - 129.126		Libres	
129.129	172.20.129.129	**Gateway para VLAN 4**	VLAN4
.129.130 - .129.254		Direcciones para las PC's de la **VLAN de DATOS** usando el DHCP de la Central Mitel	

Tabla 3.17 Detalle de Direcciones IP para la Red de Beaterio

En resumen, el diseño de VLANs con su respectivo direccionamiento, es:

RESUMEN DEL RANGO DE DIRECCIONES IP PARA CADA VLAN DE BEATERIO - PROPUESTA 2					
VLAN #	**Nombre**	**Rango Util de direcciones**	**Máscara**	**/#**	**Nro. De Clientes**
VLAN 1	VLAN de Gestion	172.20.129.1 - 172.20.129.30	255.255.255.224	/27	4
VLAN 2	VLAN de Automatización	172.20.129.33 - 172.20.129.62	255.255.255.224	/27	15
VLAN 3	VLAN de Voz	172.20.129.65 - 172.20.129.126	255.255.255.192	/26	20
VLAN 4	VLAN de Datos	172.20.129.129 - 172.20.129.254	255.255.255.128	/25	36

Tabla 3.18 Resumen de la Asignación de VLANs para la red de Beaterio

3.2.7 Elección del Tipo de asignación a VLANs en la red de la Beaterio

Al igual que para la red de la Matriz, los tipos de asignación dinámica en base a capa 3 quedan descartados por las razones antes expuestas; y el tipo de asignación dinámica en base a direcciones MAC no es factible debido a la falta de un servidor VMPS. Por lo tanto el tipo de asignación para la red de Beaterio factible y a la vez conveniente es la asignación estática de VLANs en base a puertos.

CAPITULO IV

CONFIGURACION

4.1 CONFIGURACION DE VLANs

4.1.1 VLANs Soportadas por los Switches

Tanto el switch Catalyst 3550 como el switch Catalyst 4500, soportan 1005 VLANs en los modos cliente, servidor o transparente de VTP. Las VLANs son identificadas con un número desde 1 a 4094. Los VLAN IDs desde 1002 hasta 1005 son reservados para VLANs Token Ring y FDDI. VTP solamente aprende el rango normal de VLANs, con los VLAN IDs desde 1 al 1005; los VLAN IDs mayores a 1005 son VLANs de rango extendido y no son almacenadas en el *VLAN database.* El switch debe estar en modo transparente VTP cuando se crea VLAN IDs desde 1006 a 4094. En el switch Catalyst 4500 las VLAN 0 y 4095 son solamente para uso del sistema (no pueden ser usadas ni observadas).

Los switches soportan *Per-VLAN Spanning-Tree Plus (PVST+)* y *Rapid PVST+* con un número máximo de intancias *spanning-tree*, por ejemplo de 128 para el switch Catalyst 3550, ver Tabla 4.1. Una instancia spanning-tree es permitida por VLAN. Además soportan ambos métodos de etiquetamiento *trunking*: *Inter-Switch Link (ISL)* e IEEE 802.1Q para enviar el tráfico VLAN sobre los puertos Ethernet.

En la Tabla 4.1 se muestra un resumen de las características más importantes de cada uno de los switches que se van a utilizar.

Principales Carácterísticas de los Switches Cisco Catalyst				
Carácterìstica / Switch	**Catalyst 2524 XL / 2512 XL**	**Catalyst 3524 XL**	**Catalyst 3550**	**Catalyst 4507R (Supervisor Engine IV)**
Gigabit Ethernet (fibra óptica)		X	X	X
100 Mbps Ethernet	X	X	X	X
1000 Mbps Ethernet				X
IEEE 802.1D Spanning-Tree Protocol	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 v1/v2	X	X	X	X
Número de VLANs	68	254	1005	1005
Throughput (Forwarding rate for 64bytes)	3 Mpps	6.5 Mpps	6.6 Mpps	48 Mpps
Capacidad de Backplane	3.2 Gbps	5.4 Gbps	4.4 Gbps	64 Gbps
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 Security	X	X	X	X
Port ACLs	X	X	X	X
VLAN ACLs			X	X

Tabla 4.1 Principales Característica de los Switches Cisco Catalyst

En los switches Catalyst 2900 XL y 3500 XL los VLAN IDs son desde el número 1 al 1001. La cantidad de VLANs Ethernet es 64 y 250 para los switches antes mencionados, pero si se reportan 68 ó 254 VLANs activas es porque las cuatro VLAN restantes (del 1002 a 1005) son reservadas para Token Ring y FDDI.

Nota: Un enlace troncal soporta 1005 VLANs, el protocolo de encapsulación ISL soporta 1000 VLANs y el protocolo de encapsulación 802.1Q soporta 4096 VLANs.

4.1.2 Configuración del Rango Normal de VLANs

Se puede configurar el rango normal de VLANs (con VLAN IDs desde 1 a 1005 para los switches 3550 y 4500; y con los VLAN IDs desde 1 a 1001 para los switches 2900 XL y 3500 XL) usando dos modos de configuración.

4.1.2.1 Configuración de VLAN con el Modo config-vlan

Para acceder al modo config-vlan, ingrese el comando de configuración global **vlan** con el VLAN ID. Ingrese un nuevo VLAN ID para crear una VLAN o con un VLAN ID existente para modificar la VLAN. Para mostrar la configuración VLAN, ingrese el comando de administración con privilegios **show vlan.**

Se debe usar este modo config-vlan para crear VLANs de rango extendido (VLAN ID mayor a 1005), que generalmente son VLANs para uso interno del switch.

4.1.2.2 Configuración de VLAN con el Modo de Configuración VLAN

Para acceder al modo de configuración VLAN, digite el comando de administración con privilegios **vlan database**; luego ingrese el comando **vlan** con un nuevo VLAN ID para crear una nueva VLAN o con un VLAN ID existente para modificar la VLAN. Cuando se haya finalizado la configuración, se debe ingresar el comando **apply** o **exit** para que la configuración tenga efecto. Los mensajes VTP son enviados con la información de las VLANs configuradas, a otros switches dentro del dominio VTP. En el modo servidor o transparente de VTP, la adición, cambio o eliminación de VLANs son grabadas en el archivo **vlan.dat**.

Por defecto la VLAN asignada a todos los puertos es la VLAN 1, que generalmente es la VLAN de administración de red, mientras que el nombre por defecto de las VLAN es VLANxxxx, donde xxxx representa el VLAN ID (precedida de ceros si es necesario).

4.1.3 Almacenamiento de la Configuración VLAN

Las configuraciones de los VLAN IDs del 1 al 1005 son grabadas en el archivo *vlan.dat* (VLAN database), y puede ser mostrado con el comando de administración con privilegios **show vlan**. El archivo vlan.dat se almacena en la NVRAM (nonvolatile RAM).

Para guardar el archivo *running configuration,* (que es donde se encuentra la configuración actual del switch), en el archivo *startup configuration* (el cual se graba en NVRAM) se ingresa el comando de administración con privilegios **copy running-config startup-config.**

4.1.4 Creación o Modificación de una VLAN Ethernet

La Tabla 4.2 describe como se debe crear o modificar una VLAN Ethernet con el modo config-vlan.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global
Paso 2	**vlan** *vlan-id*	Ingresar un VLAN ID, e ingresar al modo config-vlan. Digitar un nuevo VLAN ID para crear una VLAN, o ingresar un VLAN ID existente para modificar una VLAN.
Paso 3	**name** vlan-name	(Opcional) Ingresar un nombre para la VLAN. Si el nombre no es ingresado para la VLAN, por defecto es añadido el *vlan-id* encabezado por ceros, a la palabra VLAN. Por ejemplo: VLAN0004 es el nombre por defecto para la VLAN 4
Paso 4	**end**	Retornar al modo de administración con privilegios
Paso 5	**show vlan** {**name** *vlan-name* / **id** *vlan-id*}	Verificar lo configurado
Paso 6	**copy running-config starup config**	(Opcional) Si el switch está en modo transparente VTP, la configuración VLAN es guardada en el archivo running configuration tal como en el VLAN database. Este guarda la configuración en el archivo del switch startup configuration.

Tabla 4.2 Creación o Modificación de una VLAN con el Modo config-vlan[84]

Para retornar una VLAN al escenario por defecto, use el comando config-vlan: **no vlan name.**

La Tabla 4.3 muestra como se debe crear o modificar VLANs Ethernet con el modo de configuración VLAN database.

	Comando	Propósito
Paso 1	**vlan database**	Ingresar al modo de configuración VLAN database.
Paso 2	**vlan** *vlan-id* **name** *vlan-name*	Añadir una VLAN Ethernet asignando un número a esta. Si ningún nombre es ingresado para la VLAN, por defecto es añadido el vlan-id encabezado por ceros, a la palabra VLAN. Por ejemplo: VLAN0004 es el nombre por defecto para la VLAN 4
Paso 3	**apply**	Guardar los cambios realizados en el VLAN database.
Paso 4	**exit**	Actualizar el VLAN database, propagar éste a lo largo del dominio administrativo, y retornar al modo de administración con privilegios
Paso 5	**show vlan** {**name** *vlan-name* / **id** *vlan-id*}	Verificar lo configurado
Paso 6	**copy running-config starup config**	(Opcional) Si el switch está en modo transparente VTP, la configuración VLAN es guardada en el archivo running configuration tal como en el VLAN database. Este guarda la configuración en el archivo del switch startup configuration.

Tabla 4.3 Creación o Modificación de una VLAN - Modo de Configuración VLAN[85]

[84] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-8,11-9.
[85] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-9

Para retornar una VLAN al escenario por defecto, use el comando de configuración vlan: **no vlan** *vlan-id* **name.**

4.1.5 Eliminación de una VLAN

Para eliminar una VLAN con el modo config-vlan, se sigue el procedimiento que se detalla en la Tabla 4.4.

	Comando	**Propósito**
Paso 1	**configure terminal**	Ingresar al modo de configuración global
Paso 2	**no vlan** *vlan-id*	Eliminar la VLAN ingresando el VLAN ID
Paso 3	**end**	Retornar al modo de administración con privilegios
Paso 4	**show vlan brief**	Verificar la eliminación de la VLAN
Paso 5	**copy running-config starup config**	(Opcional) Si el switch está en modo transparente VTP, la configuración VLAN es guardada en el archivo running configuration tal como en el VLAN database. Este guarda la configuración en el archivo del switch startup configuration.

Tabla 4.4 Eliminación de una VLAN[86]

Para borrar una VLAN en el modo de configuración VLAN database, use el comando de administración con privilegios **vlan database,** para primero ingresar a este modo de configuración y luego el comando de configuración **no vlan** *vlan-id.*

4.1.6 Asignación de Puertos de Acceso Estático a una VLAN

Se puede asignar un puerto de acceso estático a una VLAN estando el VTP deshabilitado (modo transparente VTP).

Nota: Si se asigna una interfaz a una VLAN que no exista, la nueva VLAN es creada.

La Tabla 4.5 muestra los pasos a seguir para realizar la asignación de puertos de acceso estático a una VLAN.

[86] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-10

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global
Paso 2	**interface** *interface-id*	Ingresar a la interfaz que va a ser añadida a la VLAN
Paso 3	**switchport mode access**	Definir el modo de membresía VLAN para el puerto (puerto de acceso de capa 2)
Paso 4	**switchport access vlan** vlan-id	Asignar el puerto a una VLAN.
Paso 5	**end**	Retornar al modo de administración con privilegios
Paso 6	**show running-config interface** *interface-id*	Verificar el modo de membresía VLAN de la interfaz
Paso 7	**show interfaces** *interface-id* **switchport**	Verificar lo configurado en los campos del *Administrative Mode* y del *VLAN Access Mode* de la presentación.
Paso 8	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.5 Asignación de Puertos de Acceso Estático a una VLAN[87]

Para retornar a una interfase a su configuración por defecto, use el comando de configuración de interfaz **default interface** *interface-id*.

4.1.7 Verificación de la Configuración de VLANs

Use el comando de administración con privilegios **show vlan** para mostrar una lista de todas las VLANs en el switch, incluyendo las VLANs de rango extendidas, status, puertos e información de configuración. También se puede usar el comando EXEC **show vlan brief** para desplegar una lista de las VLANs en la base de datos con status y puertos pero sin información de configuración. Para ver las VLANs del rango normal en la base de datos VLAN (1 a 1005), usar el comando de configuración VLAN **show** (accedido por el ingreso del comando de administración con privilegios **vlan database**).

La Tabla 4.6 lista los comandos para monitorear las VLANs.

Comando	Modo del Comando	Propósito
show	VLAN configuration	Muestra el status de las VLANs en el VLAN database.
show current [*vlan-id*]	VLAN configuration	Muestra el status de todas o de la VLAN específicada en el VLAN database.
show interfaces [**vlan** *vlan-id*]	Administración con privilegios	Muestra las características de todas las interfaces o para la VLAN específicada configurada en el switch.
show running-config vlan	Administración con privilegios	Muestra todas o un rango de VLANs en el switch.
show vlan [**id** *vlan-id*]	Administración con privilegios	Muestra los parámetros de todas las VLANs o de la VLAN especificada en el switch.

Tabla 4.6 Comandos para monitorear las VLANs[88]

[87] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-11.
[88] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-15

4.2 CONFIGURACION DE VLAN TRUNKS

Las interfaces troncales Ethernet soportan diferentes modos de *trunking* (ver Tabla 4.7). Se puede setear una interfaz como *trunking*, *nontrunking* o negociar el *trunking* con la interfaz vecina. Para autonegociar el *trunking*, las interfaces deben estar en el mismo dominio VTP. La Tabla 4.7 muestra los modos de las interfaces de capa 2.

Modo	Función
switchport mode access	Pone a la interfaz (puerto de acceso) dentro de un modo permanente de nontrunking. La interfaz se convierte en una interfaz nontrunk incluso si la interfaz vecina es una interfaz troncal.
switchport mode dynamic desirable	Hace que la interfaz activamente intente convertir el enlace en un enlace troncal. La interfaz llega a ser una interfaz troncal si la interfaz vecina es seteada en el modo *trunk*, *desirable* o *auto*. El modo por defecto de un switch-port para todas las interfaces Ethernet es **dynamic desirable**.
switchport mode dynamic auto	Hace a la interfaz capaz de convertir el enlace en un enlace troncal. La interfaz llega a ser una interfaz troncal si la interfaz vecina es seteada en el modo *trunk* o *desirable*.
switchport mode trunk	Pone a la interfaz dentro de un modo permanente de trunking y negocia para convertir el enlace en un enlace troncal. La interfaz llega a ser una interfaz troncal incluso si la interfaz vecina no es una interfaz troncal.
switchport nonnegotiate	Previene que la interfaz genere tramas DTP. Se puede usar este comando solo cuando el modo de la interfaz switchport es **access** o **trunk**. Se debe manualmente configurar la interfaz vecina como una interfaz troncal para establecer una interfaz troncal.
switchport mode dot1q-tunnel	Configura la interfaz como un puerto tunel (nontrunking) a ser conectado en un enlace asimétrico con un puerto troncal 802.1Q. 802.1Q tunneling es usado para mantener la integridad de la VLAN cliente a través de una proveedor de servicio de red.

Tabla 4.7 Modos de las Interfaces de Capa 2[89]

La negociación troncal es administrada por el *Dynamic Trunking Protocol (DTP),* el cual es un protocolo punto a punto. Sin embargo, algunos dispositivos de red pueden enviar tramas DTP inadecuadas, lo cual causa configuraciones erróneas. Para evitar esto, hay que configurar las interfaces conectadas a los dispositivos que no soportan DTP a no enviar tramas DTP, es decir apagar DTP.

- Si no se pretende troncalizar a través de enlaces, entonces se debe usar el comando de configuración de interfaz **switchport mode access** para deshabilitar el *trunking*.
- Para habilitar el *trunking* a un dispositivo que no soporta DTP, usar los comandos de configuración de interfaz **switchport mode trunk** y **switchport nonnegotiate**, que causa que la intefaz llegue a ser una troncal pero sin generar tramas DTP. Además, sirve para forzar a las interfaces a ser troncales en diferentes dominios VTP.

[89] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-17.

4.2.1 Tipos de Encapsulación

Los dos protocolos de encapsulación disponibles en todas las interfaces Ethernet son: *Inter-Switch Link (ISL)* e IEEE 802.1Q. Se puede especificar cualquiera de estos dos protocolos de encapsulación o también el tipo de encapsulación puede ser autonegociado. DTP soporta autonegociación de ambos: ISL o 802.1Q.

La Tabla 4.8 lista los tipos de encapsulación troncal Ethernet.

Encapsulación	Propósito
switchport trunk encapsulation isl	Especifica la encapsulación ISL en el enlace troncal
switchport trunk encapsulation dot1q	Especifica la encapsulación 802.1Q en el enlace troncal
switchport trunk encapsulation negotiate	Especifica que la interfaz negocie con la interfaz vecina para llegar a ser una troncal ISL (preferentemente) o 802.1Q, dependiendo de la configuración y capacidad de la interfaz vecina.

Tabla 4.8 Tipos de encapsulación[90]

Nota: El switch multilayer no soporta troncales de capa 3; no se puede configurar subinterfaces o usar encapsulación en interfaces de capa 3. El switch no soporta troncales de capa 2 e interfaces VLAN de capa 3, lo cual provee capacidades equivalentes.

Nota: El actual software para los switches Catalyst 2900 XL y 3500 XL no soporta la negociación de la troncal a través del *Dynamic Trunking Protocol* (DTP).

4.2.2 Configuración VLAN de una Interfaz Ethernet de Capa 2 por Defecto

La Tabla 4.9 muestra la configuración VLAN de una interfaz Ethernet de capa 2 por defecto.

Característica	Configuración por defecto
Modo de la interfaz	**switchpor mode dynamic desirable**
Encapsulación de la troncal	**switchpor trunk encapsulation negotiate**
Rango de VLANs permitidas	VLANs de 1 a 4094
Rango de VLANs elegibles para prunning	VLANs de 2 a 1001
Default VLAN (para puertos de acceso)	VLAN 1
Native VLAN (para puertos troncales con 802.1Q)	VLAN 1

Tabla 4.9 Configuración VLAN de una Interfaz Ethernet de Capa 2 por Defecto[91]

[90] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-18.
[91] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-19.

4.2.3 Configuración de una Interfaz Ethernet como Puerto Troncal

Si se usa VTP se debe asegurar que al menos un puerto troncal es configurado sobre el switch y que éste puerto es conectado a otro puerto troncal de un segundo switch. Caso contrario no se recibirá ningún tipo de aviso VTP.

Nota: Por defecto una interfaz está en modo Capa 2. Si la interfaz vecina soporta *trunking* y está configurado para permitir *trunking*, una interfaz que está en modo Capa 3, puede llegar a ser una troncal de capa 2 cuando se ingresa el comando **switchport.**

Por defecto, las troncales negocian la encapsulación, y si la interfaz vecina soporta ambos tipos de encpasulación: ISL y 802.1Q, entonces la troncal usará la encapsulación ISL.

4.2.3.1 Configuración de un Puerto Troncal

Seguir los pasos que se muestran en la Tabla 4.10 para configurar un puerto como puerto troncal ISL o 802.1Q.

	Comando	**Propósito**
Paso 1	**configure terminal**	Ingresar al modo de configuración global
Paso 2	**interface** *interface-id*	Ingresar al modo de configuración de interfaz y el puerto a ser configurado para el trunking.
Paso 3	**switchport trunk encapsulation** {**isl** | **dot1q** | **negotiate** }	Configurar el puerto para soportar la encapsulación ISL o 802.1Q, o negociar (por defecto) con la interfaz vecina para el tipo de encapsulación. Se debe configurar cada extremo del enlace con el mismo tipo de encapsulación.
Paso 4	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk** }	Configura la interfaz como una troncal de capa 2 **dynamic auto.-** configura la interfaz como un enlace troncal si la interfaz vecina es seteada en el modo *trunk* o *desirable.* **dynamic desirable.-** configura la interfaz como un enlace troncal si la interfaz vecina es seteada en el modo *trunk* , *desirable* o *auto.* **trunk.-** configura la interfaz en modo de trunking permanente y negocia para convertir el enlace en un enlace troncal incluso si la interfaz vecina no es una interfaz troncal.
Paso 5	**switchport access vlan** *vlan-id*	(Optional) Especificar el default VLAN, el cual es usado si la interfaz detiene el trunking.
Paso 6	**end**	Retornar al modo de administración con privilegios
Paso 7	**show interfaces** *interface-id* **trunk**	Mostrar la configuración troncal de la interfaz
Paso 8	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.10 Configuración de un Puerto Troncal[92]

[92] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-20.

Para resetear todas las características *trunking* de una interfaz *trunking* a sus valores por defecto, usar el comando de configuración de interfaz **no switchport trunk.** Para deshabilitar *trunking* usar el comando de configuración de interfaz **switchport mode access** para configurar al puerto como un puerto de acceso estático. En los switches Catalyst 2900 XL y 3500 XL se utiliza el comando de configuración de interfaz **no switchport mode** para retornar al puerto al modo de acceso estático por defecto.

4.2.3.2 Definición de las VLANs permitidas sobre una troncal

Por defecto, un puerto troncal envía y recibe tráfico hacia y desde todas las VLANs. Todos los VLAN IDs, del 1 al 4094, son permitidos. Sin embargo se pueden quitar VLANs de la "lista permitida", impidiendo el tráfico de esas VLANs sobre la troncal. Para restringir el tráfico que lleva una troncal, se usa el comando de configuración de interfaz **switchport trunk allowed vlan remove** *vlan-list*, para eliminar VLANs de la "lista permitida".

Un puerto troncal puede llegar a ser un miembro de una VLAN si la VLAN es habilitada, si VTP conoce de la VLAN, y si la VLAN está en la "lista permitida". En la Tabla 4.11, se muestran los pasos para modificar la "lista permitida" en una troncal ISL o 802.1Q.

	Comando	**Propósito**
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**interface** *interface-id*	Ingresar al modo de configuración de interfaz y el puerto a ser configurado para el trunking.
Paso 3	**switchport mode trunk**	Configurar la interfaz como un puerto troncal VLAN.
Paso 4	**switchport trunk allowed vlan** {**add** | **all** | **except** | **remove**} *vlan-list*	(Opcional) Configurar la lista de VLANs permitidas sobre la troncal. El parámetro *vlan-list* es un solo número de VLAN o un rango de VLANs descrito por números VLAN, el más bajo es primero y es separado por un guión. No ingresar ningún espacio entre los parámetros VLAN separados por coma o rangos especificados con guión. Todas las VLANs son soportadas por default.
Paso 5	**end**	Retornar al modo de administración con privilegios
Paso 6	**show interfaces** *interface-id* **switchport**	Verificar lo ingresado en el campo *Trunking VLANs Enabled* de la presentación.
Paso 7	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.11Modificación de las VLANs permitidas sobre una troncal[93]

[93] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11- 21.

4.2.3.3 Cambio de la lista Pruning-Eligible

La lista *pruning-eligible* solo se aplica sobre puertos troncales. Cada puerto troncal tiene su propia lista. VTP *pruning* debe estar habilitado para que este proceso tenga efecto.

La Tabla 4.12, indica los pasos para quitar VLANs de la lista *pruning-elegible* sobre un puerto troncal.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**interface** *interface-id*	Ingresar al modo de configuración de interfaz y el puerto a ser configurado para el trunking.
Paso 3	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan* [,*vlan* [,,,]]	(Opcional) Configurar la lista de VLANs permitidas a ser recortadas (pruned) sobre la troncal. Separar los VLAN IDs no consecutivos con una coma; usar el guión para designar un rango de IDs. Las VLANs de rango extendido no pueden ser recortados (pruned). Las VLANs que son *pruning-ineligible* reciben el tráfico inundado (flooding).
Paso 4	**end**	Retornar al modo de administración con privilegios
Paso 5	**show interfaces** *interface-id* **switchport**	Verificar lo ingresado en el campo *Trunking VLANs Enabled* de la presentación.
Paso 6	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.12 Eliminación de VLANs de la lista pruning-elegible[94]

Para retornar a la lista *pruning-eligible* por defecto, se ingresa el comando de configuración de interfaz **no switchport trunk pruning vlan**.

4.2.3.4 Configuración de la VLAN Nativa para tráfico no etiquetado

Un puerto troncal configurado con etiquetado 802.1Q, puede recibir tráfico etiquetado y no etiquetado, Por defecto, el switch envía tráfico no etiquetado en la VLAN nativa configurada para el puerto. La VLAN nativa por defecto es la VLAN 1.

Nota: La VLAN nativa puede ser asignada a cualquier VLAN ID.

La Tabla 4.13, indica los pasos para configurar la VLAN nativa sobre una troncal 802.1Q.

[94] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-22.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**interface** *interface-id*	Ingresar al modo de configuración de interfaz y el puerto a ser configurado para el trunking.
Paso 3	**switchport trunk native vlan** *vlan-id*	Configurar la VLAN que va a enviar y recibir tráfico no etiquetado sobre el puerto troncal.
Paso 4	**end**	Retornar al modo de administración con privilegios
Paso 5	**show interfaces** *interface-id* **switchport**	Verificar lo ingresado en el campo *Trunking VLANs Enabled* de la presentación.
Paso 6	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.13 Configuración de la VLAN Nativa[95]

Para retornar a la VLAN nativa por defecto, VLAN 1, usar el comando de configuración de interfaz **no switchport trunk native vlan**.

Si un paquete tiene un VLAN ID igual que el VLAN ID de la VLAN nativa, entonces el paquete se enviará sin etiquetado; caso contrario, el switch envía el paquete con una etiqueta.

4.3 CONFIGURACION DEL ENRUTAMIENTO ENTRE VLANs

Por defecto, solo los hosts que son miembros de la misma VLAN pueden comunicarse. Para cambiar esto y permitir que la comunicación entre VLANs sea posible, es necesario un router o un switch de capa 3.

4.3.1 Configuración de Enrutamiento Inter-VLAN con un Router

Para que el enrutamiento entre VLANs funcione apropiadamente, todos los routers y switches involucrados deben soportar la misma encapsulación.

Para que exista enrutamiento entre VLANs en el router, se debe dividir a la interfaz que va conectada a la LAN en subinterfaces virtuales. La Tabla 4.14 muestra como se definen subinterfaces sobre una interfaz física para permitir el enrutamiento entre VLANs utilizando un router Cisco.

[95] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 11-23.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**interface FastEthernet** *slot-number/ port-number* **.** *subinterface-number*	Ingresar al modo de configuración de interfaz. El ***port-number*** identifica la interfaz física, y el ***subinterface-number*** identifica la interfaz virtual. Por lo general el *slot-number* es 0, si no existe mas de un slot en el equipo.
Paso 3	**encapsulation** {**dot1q** | **isl** | **sde** | **tr-isl**} *vlan-id*	Configurar el puerto para soportar diferentes tipos de encapsulación: 802.1Q, ISL, 802.10 o Tokeng Ring ISL. El ***vlan-id*** identifica la VLAN para la cual la subinterfaz llevará tráfico.
Paso 4	**ip address** *ip-address subnet-mask*	Ingresar la dirección IP y la máscara de subred asignadas a la subinterfaz
Paso 5	**end**	Retornar al modo de administración con privilegios
Paso 6	**show running-config**	Muestra entre otras cosas, la configuración realizada de las subinterfaces.
	copy running-config starup config	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.14 Configuración de Enrutamiento Inter-VLAN entre un Router y un Switch

4.3.2 Configuración de Enrutamiento con un Switch de Capa 3

Por defecto, el enutamiento IP está deshabilitado en el Switch Catalyst 3550. Los switches con el Standard Multilayer software Image (SMI) soportan solamente el enrutamiento por defecto, rutas estáticas y RIP. Todos los otros protocolos de enrutamiento requieren el EMI (*Enhanced Multilayer software Image*) en el switch.

Una interfaz de capa 3, puede ser de tres tipos:

- ***Routed port*:** es un puerto físico configurado como un puerto de capa 3, usando el comando de configuración de interfaz **no switchport.**
- ***Switch Virtual Interface (SVI)*:** es una interfaz VLAN creada con el comando de configuración global **interface vlan** *vlan-id* y por defecto una interfaz capa3.
- ***EtherChannel port channel* en modo Capa 3:** es una interfaz lógica port-channel ligada a la interfaz Ethernet dentro del channel group.

Un switch capa 3, puede tener una dirección IP asignada a cada routed port y SVI. Todas las interfaces de capa 3 deben tener direcciones IP asignadas. El número de routed ports y SVIs que pueden ser configurados no es limitado por software. Sin embargo, la interrelación entre este número y el número y volumen de características que han sido implementadas pueden causar un impacto en la utilización del CPU, debido a las limitaciones de hardware.

La configuración de enrutamiento en un switch de capa 3, consiste de varios importantes procedimientos:

- Soportar interfaces VLAN, crear y configurar VLANs en el switch, y asignar membresías de VLAN a interfaces de capa 2.
- Configurar interfaces de capa 3.
- Habilitar enrutamiento IP en el switch.
- Asignar direcciones IP a las interfaces de capa 3.
- Habilitar el protocolo de enrutamiento elegido en el switch.
- Configurar los parámetros del protocolo de enrutamiento (opcional).

Nota: Por defecto: no está definida ninguna dirección IP, está habilitado el enrutamiento IP classless; y el IP *default gateway*, el IP helper address y el enrutamiento IP están deshabilitados.

4.3.2.1 Asignación de direcciones IP a interfaces de capa 3

Por defecto, una SVI es creada para la *default* VLAN (VLAN 1) para permitir la administración remota del switch. Solo una interfaz virtual del switch (SVI) puede ser asociada con una VLAN, pero es necesario configurar una SVI cuando se desea enrutar entre VLANs.

La Tabla 4.15, indica los pasos para asignar una dirección IP y máscara a una interfaz virtual del switch (S*witch Virtual Interface*).

	Comando	**Propósito**
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**interface vlan** *vlan-id*	Ingresar al modo de configuración de interfaz y crear una interfaz virtual en el switch.
Paso 3	**ip address** *ip-address subnet-mask*	Configurar la interfaz con una dirección IP y una máscara de subred IP.
Paso 4	**no shutdown**	Habilitar la interfaz.
Paso 5	**end**	Retornar al modo de administración con privilegios
Paso 6	**show running-config**	Muestra entre otras cosas, la configuración realizada en la interfaz.
Paso 7	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.15 Creación de una Interfaz Virtual del Switch

Nota: Cuando una interfaz virtual del switch (SVI) es creada, ésta no llega a activarse hasta que sea asociada con un puerto físico.

Nota: Para utilizar todas las capacidades avanzadas de enrutamiento se debe instalar el EMI (*Enhanced Multilayer software Image*) en el switch.

La Tabla 4.16, indica los pasos para asignar una dirección IP y máscara a un puerto enrutado.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**interface** *interface-id*	Ingresar al modo de configuración de interfaz y especificar la interfaz de capa 3 a configurar.
Paso 3	**no switchport**	Elimina la interfaz del modo de configuración de capa 2 (si esta es una interfaz física).
Paso 4	**ip address** *ip-address subnet-mask*	Configurar la interfaz con una dirección IP y una máscara de subred IP.
Paso 5	**no shutdown**	Habilitar la interfaz.
Paso 6	**end**	Retornar al modo de administración con privilegios
Paso 7	**show interfaces** [*interface-id*] **show ip interface** [*interface-id*] **show running-config interface** [*interface-id*]	Verificar lo ingresado.
Paso 8	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.16 Configuración de un Puerto Enrutado[96]

4.3.2.2 Enrutamiento Auxiliar cuando el Enrutamiento IP está deshabilitado

Los siguientes mecanismos le permiten al switch aprender acerca de rutas de otras redes cuando no se encuentra habilitado el enrutamiento IP: Proxy ARP, *Default Gateway* e *ICMP Router Discovery Protocol (IRDP)*. El método que generalmente se va a utilizar es por *Default Gateway*, por tal razón se explica como éste se debe configurar.

Default Gateway

Este método define un *default* router o *default gateway*. Todos los paquetes no locales son enviados a este router, el cual los enruta apropiadamente o envía un IP Control Message Protocol (ICMP) redirect message hacia atrás, definiendo que ruta local debe usar el host. La limitación de este método es que no hay manera de detectar que el *default* router

[96] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 30-6

ha caído o es inalcanzable. La Tabla 4.17, muestra los pasos para definir un *default gateway* cuando el enrutamiento IP está deshabilitado.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**ip default gateway** *ip-address*	Establecer un default gateway (router).
Paso 3	**end**	Retornar al modo de administración con privilegios
Paso 4	**show ip redirects**	Muestra la dirección IP del router default gateway, para verificar lo configurado.
Paso 5	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.17 Configuración del default gateway[97]

Usar el comando de configuración global **no ip default-gateway** para deshabilitar esta función.

Nota: El comando **ip default-gateway** es utilizado cuando no se habilita el enrutamiento (**ip routing)** en los switches multilayer.

4.3.2.3 Habilitación del Enrutamiento IP Unicast

Por defecto, el switch esta en el modo de conmutación de capa 2 y el enrutamiento IP está deshabilitado. Para usar las capacidades de capa 3 del switch, se debe habilitar el enrutamiento IP. La Tabla 4.18 indica los pasos para habilitar el enrutamiento IP.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**ip routing**	Habilitar enrutamiento IP
Paso 3	**router** *ip_routing_protocol*	Especificar un protocolo de enrutamiento IP. Este paso puede incluir otros comandos, tal como especificando las redes a enrutar con el comando de configuración de router (RIP) **network.** **Nota:** El SMI soporta solamente RIP como protocolo de enrutamiento.
Paso 4	**end**	Retornar al modo de administración con privilegios
Paso 5	**show running-config**	Muestra lo ingresado
Paso 6	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.18 Habilitación del Enrutamiento IP[98]

Se usa el comando de configuración global **no ip routing** para deshabilitar el enrutamiento.

[97] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 30-11
[98] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 30-18

4.3.2.4 Configuración de Rutas Estáticas

La forma de cómo configurar rutas estáticas se muestra en la siguiente tabla.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**ip route** *destination_network sub-mask* [*next-hop* | *gateway*]	Establecer la ruta estática *destination_network* es la red a la cual se desea llegar. *sub-mask* es la máscara de la red a la cual se apunta. *next-hop* es la interfaz del router vecino más cercano hacia la red destino. *gateway* es la interfaz del propio router que apunta a la red destino.
Paso 3	**end**	Retornar al modo de administración con privilegios
Paso 4	**show ip route**	Muestra la tabla de enrutamiento, para verificar lo ingresado.
Paso 5	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.19 Configuración de rutas estáticas

4.3.2.5 Configuración de RIP

El *Routing Information Protocol (RIP)* es un *Interior Gateway Protocol (IGP)*, creado para uso de redes homogeneas y pequeñas. Este es un protocolo de enrutamiento vector distancia que usa paquetes de datos broadcast UDP (*User Datagram Protocol*) para intercambiar información de enrutamiento.

Usando RIP, el swtich envía actualizaciones de información de enrutamiento cada 30 segundos. Si el router no recibe una actualización de otro router a los 180 segundos o más, este marca a esa ruta como inusable. Y si aún no hay una actualización a los 240 segundos, el router elimina todas las entradas en la tabla de enrutamiento para este router que no ha enviado actualizaciones.

RIP utiliza el número de saltos (métrica) para evaluar las diferentes rutas. El número de saltos es el número de routers que pueden estar atravesados en una ruta. Una red directamente conectada tiene una número de saltos igual a cero; una red con un número de saltos de 16 es inalcanzable.

Si una interfaz de red no es especificada, esta no es publicada en ninguna actualización de RIP.

Configuración básica de los parámetros de RIP

En la siguiente tabla se muestran los pasos para habilitar RIP y configurar en forma básica los parámetros que se consideran importantes de este protocolo para nuestra aplicación.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**ip routing**	Habilitar enrutamiento IP
Paso 3	**router rip**	Habilitar el protocolo de enrutamiento RIP, e ingresar al modo de configuración router.
Paso 4	**network** *network number*	Asociar una red con un proceso de enrutamiento RIP. Se puede especificar múltiples comandos **network**. Las actualizaciones de enrutamiento RIP son enviadas y recibidas a través de interfaces solamente sobre estas redes.
Paso 5	**version** {**1** | **2**}	(Opcional) Configurar el switch para recibir y enviar solamente paquetes RIP versión 1 o RIP versión 2. Por default los switches reciben versión 1 y 2, pero envían solamente versión 1. También se pueden usar los comandos de interfaz **ip rip** {**send** | **receive**} **version 1** | **2** | **1 2**} para controlar que versiones son usadas para el envío y recepción de paquetes.
Paso 6	**no auto summary**	(Opcional) Deshabilita la sumarización automática. Por default, el switch sumariza subprefijos cuando cruza fronteras de red classful. Deshabilitar sumarización (solamente para RIP versión 2) para anunciar información de enrutamiento de host y subred a fronteras de red classful.
Paso 7	**end**	Retornar al modo de administración con privilegios
Paso 8	**show ip protocols**	Verificar lo ingresado
Paso 9	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.20 Configuración Básica de los parámetros de RIP[99]

Para dehabilitar el proceso de enrutamiento RIP, digitar el comando de configuración global **no router rip**. Usar el comando de administración con privilegios **show ip rip database** para ver un resumen de las direcciones entrantes en la base de datos RIP. Usar el comando de administración con privilegios **show ip route rip** para ver las rutas aprendidas por RIP; o el comando de administración con privilegios **show ip route**, para ver todas las rutas.

4.3.3 Reenvío de Paquetes Broadcast UDP y Protocolos

La razón por la cual se explica el envío de paquetes broadcast UDP y protocolos es porque las peticiones y respuestas DHCP son paquetes UDP (*User Datagram Protocol*).

[99] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 30-20, 30-21.

Normalmente los paquetes UDP no son enviados a otro segmento de red, (en donde se puede encontrar el servidor DHCP). Para solucionar esta situación se configura a una interfaz del router para enviar cierta clase de broadcast a un *helper address* (en este caso será la dirección del servidor DHCP). Puede existir más de un *helper address* por interfaz.

Se pueden especificar múltiples protocolos UDP. También se puede especificar el protocolo *Network Disk (ND)*, el cual es usado por estaciones de trabajo más antiguas *diskless Sun* y el protocolo de seguridad de red SDNS. Por defecto, el envío de UDPs y NDs son habilitados si se ha definido un *helper address* para una interfaz.

Si no se especifica ningún puerto UDP cuando se configura el envío de broadcast UDP, entonces se está configurando al dispositivo de capa 3 a actuar como un agente de envío BOOTP. Los paquetes BOOTP llevan la información DHCP.

La Tabla 4.21 indica los pasos para habilitar el envío de paquetes broadcast UDP sobre una interfaz y especificar la dirección de destino.

	Comando	**Propósito**
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**interface** *interface-id*	Ingresar al modo de configuración de interfaz y especificar la interfaz de capa 3 a configurar.
Paso 3	**ip helper-address** *address*	Habilitar el reenvío y especificar la dirección de destino para el reenvío de paquetes broadcast UDP, incluyendo BOOTP.
Paso 4	**exit**	Retornar al modo de configuración global.
Paso 5	**ip forward-protocol** {**udp** [*port*] | **nd** | **sdns**}	Especificar que protocolos el router envía cuando reenvía los paquetes broadcast.
Paso 6	**end**	Retornar al modo de administración con privilegios
Paso 7	**show ip interface** [*interface-id*] **show running-config**	Verificar lo ingresado en la interfaz o en todas las interfaces.
Paso 8	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.21 Reenvío de paquetes broadcast UDP[100]

4.3.4 Configuración del Agente de Relevo DHCP (DHCP Relay Agent)

Por defecto el agente de relevo DHCP en el switch de capa 3 se encuentra habilitado. El agente de relevo DHCP envía los paquetes entre los clientes y servidores, cuando ellos no se encuentran en la misma red física. El DHCP Relay Agent es configurado con un

[100] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 30-15.

helper address para habilitar el envío de broadcast y la transferencia de mensajes DHCP entre los clientes y el servidor. La Tabla 4.22 muestra el procedimiento para configurar el DHCP Relay utilizando VLANs.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**interface vlan** *vlan-id*	Ingresar al modo de configuración de interfaz y crear una interfaz virtual de switch
Paso 3	**ip helper-address** *address*	Especificar la dirección de reenvío de paquetes DHCP. El helper-address puede ser una dirección de servidor DHCP específica, o puede ser la dirección de red si otros servidores DHCP están sobre el segmento de red destino.
Paso 4	**exit**	Retornar al modo de configuración global.
Paso 5	**interface range** *port-range* *o* **interface** *interface-id*	Configurar los múltiples puertos físicos que están conectados a los cliente DHCP, e ingresar al modo de configuración de rango de interfaces o Configurar un solo puerto físico que está conectado al cliente DHCP, e ingresar al modo de configuración de interfaz.
Paso 6	**switchpor mode access**	Definir el modo de membresía VLAN para el puerto.
Paso 7	**switchpor access vlan** *vlan-id*	Asignar los puertos a la misma VLAN que está configurada en el paso 2.
Paso 8	**end**	Retornar al modo de administración con privilegios
Paso 9	**show running-config**	Verificar lo configurado.
Paso 10	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.22 Configuración del DHCP Relay utilizando VLANs[101]

Para eliminar el envío de mensajes de DHCP a una dirección específica, digitar el comando de configuración global **no ip helper-address** *address*.

4.4 CONFIGURACION DE VLAN TRUNKING PROTOCOL (VTP)

La Tabla 4.23 muestra la configuración VTP por defecto.

Característica	Configuración por defecto
Nombre del dominio VTP	Nulo
Modo VTP	Server
Estado habilitado de la versión 2 de VTP	Versión 2 es deshabilitada
Password de VTP	Ninguno
VTP pruning	Deshabilitado

Tabla 4.23 Configuración VTP por defecto[102]

Se pueden usar dos modos de configuración VTP:

a) Configuración VTP en el Modo de Configuración Global

[101] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 18-6.
[102] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 12-6.

b) Configuración VTP en el Modo de Configuración VLAN

En ambos modos de configuración VTP, la información VTP es almacenada en el VTP VLAN database (vlan.dat). Cuando el modo VTP es transparente, el nombre y modo de dominio VTP son guardados en el archivo running configuration, y se puede almacenar en el archivo startup configuration con el comando de administración con privilegios **copy running-config statup-config.** Tanto el nombre de dominio, password y versión de VTP deben ser los mismos en todos los switches para que intercambien la información VTP.

4.4.1 Configuración del Servidor VTP

La Tabla 4.24 indica los pasos para que un switch sea un Servidor VTP, usando el modo de configuración global.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**vtp mode server**	Configurar al switch para el modo servidor VTP (por default).
Paso 3	**vtp domain** *domain-name*	Configurar el nombre del dominio de administración VTP. El nombre puede ser de 1 a 32 caracteres.
Paso 4	**vtp password** *password*	(Opcional) Configurar el password para el dominio VTP. El password puede ser de 8 a 64 caracteres.
Paso 5	**end**	Retornar al modo de administración con privilegios
Paso 6	**show vtp status**	Verificar lo ingresado en los campos *VTP Operating Mode* y el *VTP Domain Name* en la presentación

Tabla 4.24 Configuración del Servidor VTP con Modo de Configuración Global[103]

La Tabla 4.25 indica los pasos para que un switch sea un Servidor VTP, usando el modo de configuración VLAN.

	Comando	Propósito
Paso 1	**vlan database**	Ingresar al modo de configuración VLAN.
Paso 2	**vtp server**	Configurar al switch para el modo servidor VTP (por default).
Paso 3	**vtp domain** *domain-name*	Configurar el nombre del dominio de administración VTP. El nombre puede ser de 1 a 32 caracteres.
Paso 4	**vtp password** *password*	(Opcional) Configurar el password para el dominio VTP. El password puede ser de 8 a 64 caracteres.
Paso 5	**end**	Retornar al modo de administración con privilegios
Paso 6	**show vtp status**	Verificar lo ingresado en los campos *VTP Operating Mode* y el *VTP Domain Name* en la presentación

Tabla 4.25 Configuración del Servidor VTP con Modo de Configuración VLAN[104]

[103] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 12-9.
[104] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 12-10.

4.4.2 Configuración del Cliente VTP

La Tabla 4.26 indica los pasos para que un switch sea un Cliente VTP, usando el modo de configuración global.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**vtp mode client**	Configurar al switch para el modo cliente VTP.
Paso 3	**vtp domain** *domain-name*	Configurar el nombre del dominio de administración VTP. El nombre puede ser de 1 a 32 caracteres.
Paso 4	**vtp password** *password*	(Opcional) Configurar el password para el dominio VTP. El password puede ser de 8 a 64 caracteres.
Paso 5	**end**	Retornar al modo de administración con privilegios
Paso 6	**show vtp status**	Verificar lo ingresado en los campos *VTP Operating Mode* y el *VTP Domain Name* en la presentación

Tabla 4.26 Configuración del Cliente VTP con Modo de Configuración Global[105]

También se puede configurar un cliente VTP con el comando de administración con privilegios **vlan database** para ingresar al modo de configuración VLAN e ingresando el comando **vtp client.**

4.4.3 Configuración del Modo Transparente VTP

Cuando se configura al switch en modo transparente VTP, quiere decir que se deshabilita VTP en el switch.

La Tabla 4.27 muestra la configuración del modo transparente VTP con el modo de configuración global.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**vtp mode transparent**	Configurar al switch para el modo transparente VTP (deshabilita VTP).
Paso 3	**end**	Retornar al modo de administración con privilegios
Paso 4	**show vtp status**	Verificar lo ingresado en los campos *VTP Operating Mode* y el *VTP Domain Name* en la presentación
Paso 5	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración. **Nota:** Solamente el modo VTP y el nombre del dominio son guardados en el switch running configuration y puede ser copiado en el archivo startup configuration.

Tabla 4.27 Configuración del VTP Transparente con Modo de Configuración Global[106]

[105] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 12-11.
[106] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 12-12.

También se puede configurar el modo transparente VTP con el comando de administración con privilegios **vlan database** para ingresar al modo de configuración VLAN e ingresando el comando **vtp transparent.**

Para retornar a un estado de no password, se digita el comando de configuración global o comando de configuración VLAN **no vtp password**, y si me encuentro en el modo cliente o transparente VTP puedo retornar al modo por defecto que es el de Servidor VTP con el comando de configuración global **no vtp mode,** o con los comandos de configuración VLAN **no vtp client** y **no vtp transparent**, respectivamente.

4.4.4 Habilitación de VTP Versión 2

Un switch en modo transparente VTP con la versión 1 de VTP, no envía actualizaciones VTP y no actúa sobre las actualizaciones recibidas de otros switches. Sin embargo, con la versión 2 de VTP, envía todos los avisos VTP recibidos en todos sus enlaces troncales. Solo se puede configurar la versión en los switches que están en modo servidor o transparente VTP.

Las versiones 1 y 2 de VTP no son interoperables dentro de un mismo dominio VTP. No habilitar la versión 2 de VTP a menos que todos los switches en el dominio VTP soporten la versión 2. La Tabla 4.28 muestra la habilitación de la versión 2 de VTP.

	Comando	**Propósito**
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**vtp version 2**	Habilitar la versión 2 de VTP en el swtich.
Paso 3	**end**	Retornar al modo de administración con privilegios
Paso 4	**show vtp status**	Verificar que la versión 2 de VTP está habilitado en el campo *VTP V2 Mode* de la presentación.

Tabla 4.28 Habilitación de la versión 2 de VTP[107]

Para deshabilitar la versión 2 de VTP, usar el comando de configuración global **no vtp versión**. También se puede habilitar la versión 2 de VTP con el comando de administración con privilegios **vlan database** para ingresar al modo de configuración VLAN e ingresando el comando **vtp v2-mode.** Para deshabilitar la versión 2 de VTP, se utiliza el comando de configuración VLAN **no vtp v2-mode.**

[107] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 12-13

4.4.5 Habilitación de VTP Pruning

La Tabla 4.29 muestra la habilitación de VTP *pruning.*

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**vtp pruning**	Habilitar pruning en el dominio administrativo VTP. Por defecto, pruning está deshabilitado. Se necesita hablitar pruning solamente sobre el switch en modo servidor VTP.
Paso 3	**end**	Retornar al modo de administración con privilegios
Paso 4	**show vtp status**	Verificar que la versión 2 de VTP está habilitado en el campo *VTP V2 Mode* de la presentación.

Tabla 4.29 Habilitación de VTP Pruning[108]

Para deshabilitar VTP *Pruning*, usar el comando de configuración global **no vtp pruning**. También se puede habilitar VTP *Pruning* con el comando de administración con privilegios **vlan database** para ingresar al modo de configuración VLAN e ingresando el comando **vtp pruning.** Para deshabilitar VTP *Pruning*, se utiliza el comando de configuración VLAN **no vtp pruning.**

4.4.6 Monitoreo de VTP

Se monitorea VTP desplegando la información de configuración VTP: el nombre de dominio, la revisión VTP actual y el número de VLANs. También se puede desplegar las estadísticas acerca de los avisos enviados y recibidos por el switch. La Tabla 4.30 muestra los comandos para monitorear VTP.

Comando	Propósito
show vtp status	Muestra la información de configuración VTP en el switch
show vtp counters	Muestra los contadores acerca de los mensajes VTP que han sido enviados y recibidos.

Tabla 4.30 Monitoreo de VTP[109]

4.4.7 Añadiendo un Switch Cliente VTP a un Dominio VTP

Antes de añadir un cliente VTP a un dominio, siempre se debe verificar que el número de revisión de configuración VTP sea más bajo que el número de revisión de configuración de los otros switches en el dominio VTP. Si sucede lo contrario, éste switch

[108] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 12-13.
[109] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 12-15.

que se añade puede borrar toda la información VLAN del servidor VTP y del dominio VTP.

La Tabla 4.31 indica los pasos para verificar y resetear el número de revisión de configuración VTP en el switch antes de añadirlo al dominio VTP.

	Comando	Propósito
Paso 1	**show vtp status**	Chequear el número de revisión de VTP Si el número es 0, añadir el switch al dominio VTP. Si el número es mayor a 0, anotar el nombre del dominio y el número de revisión de configuración, y continuar con los proximos pasos para resetear el número de revisión de configuración.
Paso 2	**configure terminal**	Ingresar al modo de configuración global.
Paso 3	**vtp domain** *domain-name*	Cambiar el nombre del dominio mostrado en el paso 1 a un nuevo nombre.
Paso 4	**end**	La información VLAN en el switch es actualizada y el número de revisión de configuración es reseteado a 0. Y se retorna al modo de administración con privilegios.
Paso 5	**show vtp status**	Verificar que el número de revisión de configuración ha sido reseteado a 0.
Paso 6	**configure terminal**	Ingresar al modo de configuración global.
Paso 7	**vtp domain** *domain-name*	Ingresar el nombre del dominio original en el switch.
Paso 8	**end**	La información VLAN en el switch es actualizada y se retorna al modo de administración con privilegios.
Paso 9	**show vtp status**	(Opcional) Verificar que el nombre del dominio es el mismo que en el paso 1 y que el número de revisión de configuración es 0.

Tabla 4.31 Verificación y Cambio del Número de Revisión de VTP[110]

También se puede cambiar el nombre del dominio VTP con el comando de administración con privilegios **vlan database** para ingresar al modo de configuración VLAN e ingresando el comando **vtp domain** *domain-name***.** En este modo, se debe ingresar el comando **exit** para actualizar la información y retornar al modo de administración con privilegios.

4.5 CONFIGURACIÓN DE SPANNING-TREE (STP)

Debido a que tanto en la red de la Matriz como en la red de Beaterio se utilizan switches Catalyst 3500 XL e incluso 2900 XL, (de acuerdo a los diseños de red propuestos), que solo soportan el modo PVST+ y no otros modos como en los switches Catalyst 3550 y 4500, se decidió solo habilitar el modo PVST+ en todos los switches, como se muestra a continuación.

[110] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 12-14.

4.5.1 Configuración del Modo Spanning-Tree

Esta elección se realiza en los switches Catalyst 3550 y 4500, porque en los switches Catalyst 3500 XL y 2900 XL, por defecto ya está habilitado PVST+.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**spanning-tree mode** {**pvst** | **mst** | **rapid-pvst**}	Configurar un modo spanning-tree: Seleccione **pvst** para habilitar PVST+ (por default) Seleccione **mst** para habilitar MST (y RSTP) Seleccione **rapid-pvst** para habilitar PVST+.
Paso 3	**end**	Retornar al modo de administración con privilegios
Paso 4	**show spanning-tree summary** y **show spanning-tree interface** *interface-id*	Verificar lo ingresado
Paso 5	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.32 Configuración del Modo STP[111]

4.5.2 Deshabilitación de Spanning-Tree

STP está habilitado por defecto en la VLAN 1 y en todas las nuevas VLANs creadas, hasta el número máximo de instancias STP permitidas sobre el switch (Ver Tabla 4.1 Principales Característica de los Switches Cisco Catalyst). La siguiente tabla muestra como deshabilitar spanning-tree por VLAN.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**no spanning-tree vlan** vlan-id	Deshabilitar spanning-tree por VLAN. Para *vlan-id,* se puede especificar una sola VLAN identificada por el número de VLAN ID, un rango de VLANs separadas por un guión, o una serie de VLANs separadas por una coma.
Paso 3	**end**	Retornar al modo de administración con privilegios
Paso 4	**show spanning-tree vlan** *vlan-id*	Verificar lo ingresado
Paso 5	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.33 Deshabilitación de STP por VLAN[112]

4.5.3 Configuración del Switch Raíz

El switch raíz o *root switch*, puede ser seleccionado utilizando el comando que se muestra en la Tabla 4.34, el cual cambia el *switch priority* desde el valor por defecto

[111] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 15-13.
[112] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 15-14.

32768 a un valor significativamente mas bajo, como 24576 si se utiliza el *extended system ID*, o a 8192 si no se utiliza esta opción.

Si se utiliza el *extended system ID*, y se setea a cada VLAN para que el mismo switch, sea el switch raíz, entonces cada VLAN tendrá su propio *bridge ID* a partir del valor 24576.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**no spanning-tree vlan** vlan-id **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Configurar el switch para que llegue a ser la raíz de la VLAN especificada. Para *vlan-id* , se puede especificar una sola VLAN identificada por el número de VLAN ID, un rango de VLANs separadas por un guión, o una serie de VLANs separadas por una coma. (Opcional) Para **diameter** *net-diameter,* especificar el número máximo de switches entre dos estaciones finales cualquiera. El rango es de 1 a 7. (Opcional) Para **hello** *seconds* , especificar el intervalo en segundos entre la generación de mensajes de configuración del root switch. El rango es de 1 a 10 segundos, por default es 2 segundos. **Nota:** Cuando se ingresa este comando sin las palabras opcionales, el switch recalcula el forward-time, hello-time, max-age y prioridad. Si previamente se han configurado estos parámetros, el switch los recalcula.
Paso 3	**end**	Retornar al modo de administración con privilegios
Paso 4	**show spanning-tree detail**	Verificar lo ingresado
Paso 5	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.34 Configuración del Switch Raíz primario[113]

También se puede configurar *root switches* de respaldo con el comando de configuración global: **spanning-tree vlan** *vlan-id* **root secondary.**

4.5.4 Configuración de la Prioridad del Switch

La prioridad del switch también puede ser configurada directamente, para que éste se convierta en el switch raíz, como se muestra en la Tabla 4.35. Aunque se recomienda mejor utilizar los comandos antes mencionados.

[113] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 15-16.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**spanning-tree vlan** vlan-id **priority** *priority*	Configurara la prioridad del switch para una VLAN Para *vlan-id* , se puede especificar una sola VLAN identificada por el número de VLAN ID, un rango de VLANs separadas por un guión, o una serie de VLANs separadas por una coma. Para *priority* el rango es de 0 a 61440 en incrementos de 4096; por default es 32768. El switch con la prioridad mas baja es elegido como el root switch. Los valores de prioridad válidos son: 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, y 61440. Otros valores serán rechazados.
Paso 3	**end**	Retornar al modo de administración con privilegios
Paso 4	**show spanning-tree vlan** *vlan-id*	Verificar lo ingresado
Paso 5	**copy running-config starup config**	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.35 Configuración de la Prioridad de Switch[114]

4.5.5 Verificación del Status de Spanning-Tree

La siguiente tabla muestra comandos que ayudan a visualizar el status de STP.

Comando	Propósito
show spanning-tree active	Muestra la información spannig-tree solamente en interfaces activas
show spanning-tree detail	Muestra un resumen detallado de la información de interfaz
show spanning-tree interface *interface-id*	Muestra información spannig-tree para la interfaz especificada.
show spanning-tree summary [**totals**]	Muestra un resumen de los estados de los puertos o muestra todas las líneas de la sección del estado STP.

Tabla 4.36 Verificación del Status de STP[115]

4.6 CONFIGURACIÓN BASICA DE CALIDAD DE SERVICIO

Los switches Cisco Catalyst 2900 XL y 3500 XL si proveen calidad de servicio (Qos) en base a los valores de clase de servicio (CoS) del estándar IEEE 802.1p, como se indica a continuación: las tramas con un valor de prioridad de 0 al 4, son enviados al encolamiento de prioridad normal; mientras que las tramas con un valor de prioridad de 5 al 7, son enviados al encolamiento de alta prioridad.

En los switches Cisco Catalyst 3550 y 4500 se debe primeramente habilitar la calidad de servicio en todo el switch, y luego utilizar el comando de configuración de interfaz **mls**

[114] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 15-18.
[115] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 15-24.

qos trust cos, para confiar en los valores de clase de servicio (CoS), enviados por los teléfonos IP. Este procedimiento se muestra en la Tabla 4.37.

	Comando	Propósito
Paso 1	**configure terminal**	Ingresar al modo de configuración global.
Paso 2	**mls qos**	Habilitar QoS global.
Paso 3	**interface** *interface-id*	Ingresar al modo de configuración de interfaz y especificar la interfaz que dará confianza (trusted). Interfaces válidas incluyen interfaces fisicas.
Paso 4	**mls qos trust cos**	Configurar el estado de confianza del puerto. Por default, el puerto no da confianza. **cos .-** clasifica los paquetes que ingresan con los valores Cos del paquete. Para paquetes no etiquetados, el valor CoS por default del puerto es usado. El valor CoS por default del puerto es 0. Use la palabra **cos** si la red está compuesta de LANs Ethernet, switches Catalyst 3500 XL y Catalyst 2900XL y no tiene más de dos tipos de tráfico. Recordar que en los switches Catalyst 3500 XL y Catalyst 2900XL, CoS configura cada puerto que está transmitiendo con una cola de transmisión de prioridad normal y una cola de transmisión de alta prioridad.
Paso 5	**end**	Retornar al modo de administración con privilegios
	show mls qos interface	Verificar lo ingresado
	copy running-config starup config	(Opcional) Guardar los cambios realizados en el archivo de configuración.

Tabla 4.37 Configuración básica de Calidad de Servicio[116]

4.7 CONFIGURACIÓN DE LOS ROUTERS DE ACCESO

Dependiendo de la red y de sus respectivos diseños propuestos, en cada uno de los routers que ofrecen los diferentes accesos, se deben cambiar las direcciones IP, máscaras e incluso habilitar correctamente los protocolos de enrutamiento necesarios.

4.7.1 Configuración de la Interfaz LAN del Router Vanguard Motorola

Es necesario utilizar un protocolo de enrutamiento, entre el router que pertenece a la Frame Relay y el switch multilayer (ya sea el switch Catalyst 4500 o el switch Catalyst 3550) que realiza la conmutación de VLANs definidas en la red de área local, para que éste último conozca las rutas que integrarán a esta red local con el resto de la red de Petrocomercial; o lo que es más importante, en redes como la de Beaterio que no tiene sus propios servidores, ésta necesita conocer las rutas para llegar a los servidores que se encuentran en la red de la Matriz. Es por esta razón que debemos saber como se configura

[116] Tabla del Catalyst 3550 Multilayer Switch Software Configuration Guide, Chap-Pág. 13-4

RIP versión 2, (versión de RIP seleccionada por sus características mejoradas) sobre la interfaz LAN o Ethernet del router Vanguard Motorota.

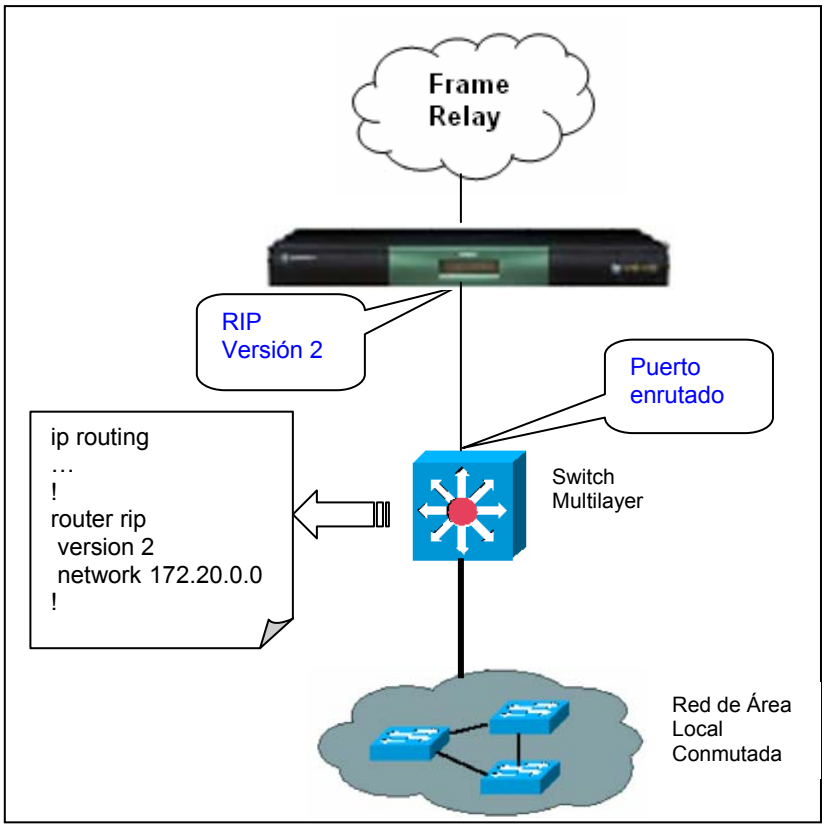


Figura 4.1 Configuración de la Interfaz LAN del Router Vanguard

En primer lugar debemos verificar que esté habilitado RIP en el Router. Desde el menú principal del router se eligen las siguientes opciones: **Configure -> Configure Router -> Configure IP -> Parameters**. En la opción **RIP Enable** digitar **Enable**, para habilitar el protocolo de enrutamiento RIP en todo el router.

```
Configure IP Parameters
…
RIP Enable: Enabled/
…
```

A continuación se configura la interfaz Ethernet del router de la siguiente manera:

Una vez en el menú principal del router se seleccionan las siguientes opciones: **Configure -> Configure Router -> Configure IP -> Interfaces.**

Luego se configuran las opciones: **número de interfaz**, **dirección IP** y **máscara**, de acuerdo al direccionamiento IP ya establecido. Por lo general el número de interfaz es 1.

```
Configure IP Interface Configuration Table

[1] Interface Number: 1/
[1] IP Address : 172.20.129.11/
[1] IP Address Mask: 255.255.255.224/
…
```

Nota: Recordar que en el Router Vanguard Motorota, las interfaces LAN usan desde la interfaces 1 a la 4 y desde la 5 a la 255 son para interfaces WAN.

A continuación se detalla como deben ser configuradas las opciones o banderas de RIP sobre la interfaz LAN del router Vanguar Motorola:

```
Configure IP Interface Configuration Table
…
[1] Accept RIP: VER2/
[1] RIP metric: 1/
[1] Send RIP Version: VER2_M/
[1] Send Aggregated Routes: Disabled/
[1] Authentication Type: None/
[1] Periodic Broadcast Interval: 30/
[1] Route Invalid Time: 180/
[1] Route Flush Time: 300/
[1] Route Hold Down Time: 240/
[1] Learn Network Routes: Enabled/
[1] Learn Subnet Routes: Enabled/
[1] Override Default Route: Disabled/
[1] Override Static Routes: Disabled/
[1] Advertise Default Route: Disabled/
[1] Advertise Network Routes: Enabled/
[1] Advertise Subnet Routes: Enabled/
[1] Advertise Static Routes: Enabled/
[1] Advertise Direct Routes: Enabled/
[1] IP RIP Split Horizon: With_Poison_Reverse/
…
```

El significado de cada una de las opciones o banderas más importantes de RIP es:

- ***Accept RIP***, especifica la versión de los paquetes de RIP que se van a recibir en el router sobre esta interfaz. Versión 1, versión 2, ambas, o deshabilitar.
- ***RIP metric***, especifica el número de saltos para recibir un paquete a través de esta interfaz. Del 1 al 15.
- ***Send RIP***, especifica la versión de los paquetes RIP con la que van a ser enviados sobre esta interfaz. Versión 1, versión 2 como multicast (VER2_M), versión 2 como broadcast (VER2_B).

- ***Periodic Broadcast Interval***, especifica en segundos cada que tiempo será enviada la tabla de enrutamiento.
- ***Route Invalid Time***, especifica el tiempo en segundos, después del cual una ruta expirará, si no se han recibido actualizaciones RIP, y será la ruta marcada como borrada.
- ***Route Flush Time***, especifica el tiempo en segundos, después del cual una ruta será borrada de la tabla de enrutamiento.
- ***Learn Network Routes*****,** habilita o deshabilita el aprendizaje de nuevas rutas de red recibidas desde routers vecinos.
- ***Learn Subnet Routes*****,** habilita o deshabilita el aprendizaje de nuevas rutas de subredes recibidas desde routers vecinos.
- ***Override Defualt Route*****,** permite habilitar o deshabilitar el pasar por alto el *default gateway* configurado, en caso que se reciba una actualización RIP que anuncia una ruta por defecto con un menor costo.
- ***Override Static Routes*****,** permite habilitar o deshabilitar el pasar por alto las rutas estáticas ya configuradas, en caso que se reciba una actualización RIP que anuncia rutas estáticas con menor costo.
- ***Advertise Default Route*****,** Habilita o deshabilita el anuncio de la ruta por defecto.
- ***Advertise Network Routes*****,** Habilita o deshabilita los anuncios RIP de rutas de red para esta interfaz.
- ***Advertise Subnet Routes*****,** Habilita o deshabilita los anuncios RIP de rutas de subred para esta interfaz.
- ***Advertise Static/Direct Routes*****,** Habilita o deshabilita los anuncios RIP de rutas estáticas y rutas directamente conectadas a esta interfaz.
- ***IP RIP Split Horizont*****,** Habilita RIP Split Horizont, que previene que las rutas sean anunciadas sobre la misma interfaz que ellas fueron aprendidas. Con Poison_Reverse significa que las rutas si son anunciadas sobre la misma interfaz que fueron aprendidas, pero contiene una métrica de infinito (16).

Otra opción que no es parte de RIP, pero si es parte de la configuración de la interfaz, es la opción **VLAN ID,** que es el identificador VLAN que se utiliza para enviar los paquetes sobre esta interfaz, pero debido a que se conecta a un puerto enrutado (o puerto

conmutado de acceso a la VLAN 1, dependiendo del diseño seleccionado) de un switch multilayer, entonces no es necesario manipular esta opción y por consiguiente se deja el valor por defecto que es 1.

```
Configure IP Interface Configuration Table
…
[1] VLAN ID: 1/
…
```

Otra opción que es importante validar es el tipo de encapsulación que está utilizando la interfaz LAN del router, y de acuerdo a lo establecido esta interfaz no debe tener ningún tipo de encapsulación, debido a que la interfaz con la que se conecta con el switch multilayer es un puerto enrutado o conmutado de acceso a la VLAN 1 (dependiendo del diseño seleccionado).

Para llegar a esta opción seguimos los siguientes pasos: **Configure -> Port.** Y elegimos el puerto 5 que es el Ethernet, y seteamos la opción **Encapsulation** como **None**.

```
Configure Port

Port Number: 1/5
[5] *Port Type: ETH/
…
[5] VLAN Encapsulation: None/
…
```

4.7.2 Configuración de Rutas Estáticas en el Router Vanguard Motorota

Para configurar los parámetros de una ruta estática se debe seguir la siguiente secuencia de opciones: **Configure -> Configure Router -> Configure IP -> Static Route**

Los siguientes parámetros forman la tabla de rutas IP, la cual es utilizada para definir las rutas estáticas:

- ***Entry Number*:** Es el número de la ruta estática dentro de la tabla de rutas IP. De 1 a 1024, por defecto es 1.
- ***IP Network/Subnet*:** Es la dirección IP de la red destino. Por defecto es 0.0.0.0

- ***IP Mask*:** Especifica la máscara IP, que define la dirección de subred de la red destino. Por defecto es 255.255.255.0
- ***Next Hop*:** Es la dirección del próximo salto hacia el destino especificado. Por defecto es 0.0.0.0
- ***Metric*:** Especifica la distancia o costo hacia el destino. Este es interpretado como el número de saltos.

4.7.3 Configuración de Rutas e Interfaz LAN de los Routers IBMs

Los routers IBM que se utilizan en la Matriz y en los diferentes lugares remotos, solamente utilizan rutas estáticas, por lo tanto solo es necesario saber como configurar: estas rutas estáticas, la dirección IP de la interfaz LAN y su respectiva máscara.

Una vez que se ingresa al router IBM (*), ya sea el 2216 o el 2216-400, para ingresar al modo de configuración del router (>), se digita **Talk 6:**

```
2216 *talk 6
2216 IP config>
```

Nota: Para ver el menú del router IBM en cualquier opción seleccionada, se ingresa el símbolo de pregunta "**?**". Y para ver las sub-opciones de una opción disponible se escribe esa opcion + el símbolo de pregunta "?".

```
2216 IP config>list ?
ALL
…
VRID
```

Nota: En el router IBM 2216-400 para disponer de las opciones de cambio o adición de dirección IP, máscara y rutas estáticas, primero se debe ingresar **protocol IP.**

```
2216-400 Config>protocol IP
2216-400 IP config>?
```

Los comandos que se detallan a continuación son los mismos tanto para el router IBM 2216 como para el router IBM 2216-400.

Para configurar la dirección IP y máscara se digita: **{change | add} address**, luego se selecciona que interfaz se va a configurar, y se setea finalmente los datos deseados, como se muestra a continuación:

```
2216 IP config>add address
Which net is this address for [0]? 0
New address []? 172.20.65.2
Address mask [255.0.0.0]?255.255.255.0
```

Para ver la dirección configurada se elige la opción **List address.**

```
2216 IP config>list address
IP addresses for each interface:
  intf    0   172.20.64.2      255.255.248.0    Local wire broadcast, fill 1
  intf    1   172.20.64.3      255.255.248.0    Local wire broadcast, fill 1
  …
  intf   24   172.20.32.25     255.255.255.252  Local wire broadcast, fill 1
  intf   25                          IP disabled on this interface
Internal IP address: 172.20.64.2
```

Para configurar una ruta estática se digita **{change | add} route**, y se completan los siguientes parámetros:

```
2216 IP config>add route
IP destination []? 172.20.0.0
Address mask [255.0.0.0]? 255.255.0.0
Via gateway 1 at []? 172.20.65.151
Cost [1]?
Via gateway 2 at []?
```

En el parámetro ***IP destination*** va la dirección de red destino, es decir la red que deseo alcanzar o con lo cual quiero comunicarme, y en ***Address mask*** la respectiva máscara de esta red. En ***Via gateway 1 at*** va la dirección de una de las interfaces del router o la dirección del próximo salto a través del cual se llega a la red destino, y en ***Cost*** se indica el costo hacia este *gateway*.

Para ver las rutas creadas se digita **List route.**

```
2216 IP config>list route

route to 172.20.97.0    ,255.255.255.0   via 172.20.32.10    cost 1
route to 172.20.0.0     ,255.255.0.0     via 172.20.65.151   cost 1
route to 172.20.139.0   ,255.255.255.0   via 172.20.32.17    cost 1
route to 172.20.140.0   ,255.255.255.0   via 172.20.32.13    cost 1
route to 172.20.77.0    ,255.255.255.0   via 172.20.32.5     cost 1
```

4.8 CONFIGURACIÓN DEL CONTROLADOR DE LA CENTRAL IP MITEL

4.8.1 Configuración de la dirección IP del Controlador RTC

Primeramente debe existir una conexión serial entre la PC que da el mantenimiento y el Controlador.

1. Iniciar el programa de comunicación en la PC, éste puede ser el Hyper Terminal de Windows.
2. Presionar el botón de **Reset** del Controlador (usar un objeto afilado no metálico).
3. Cuando el programa de comunicación muestra: ***Press any key to stop auto-boot***, presione una tecla.
4. Cuando se muestre **[VxWorks Boot]**:, digite "**c"** y presione ENTER.
5. Luego pasa por la configuración VxWorks (que se muestra en la Tabla 4.38). Por cada línea de configuración en **negrilla**, ingrese un valor, luego presione ENTER. Para el resto de valores de configuración, presione ENTER para aceptar el valor por defecto.

   Nota: El PC de mantenimiento debe estar en la misma subred que el controlador

   Nota: No rellenar con ceros en las direcciones IP.

Configuración VxWorks

Prompt	**Valor**	**Nota**
boot device	ata=0, 0	El dispositivo Boot es el disco
processor number	0	No usado
host name	bootHost	
file name	/sysro/Rtc8260	Localización del Boot y el nombre del archivo
inet on ethernet (e)		**Dirección IP y máscara de subred (hex) para el Controlador RTC (por ejemplo, 134.199.63.11:ffffff00). Obtener esto de su administrador IT.**
inet on backplane (b)		
host inet (h)		Dirección IP del PC. Usado para actualizaciones de sofware
gateway inet (g)		**Dirección IP del default gateway del usuario final para el 3300 ICP (debe estar fuera del rango del DHCP)**
user (u)	**ftp**	
ftp password (ftp)	**ftp**	
flags (f)	0x0	Dirección IP fija (0x40 usado sobre el E2T para el DHCP)
target name (n)		
startup script (s)		
other (o)	motfcc	Otro dispositivo, E2T usado desde el Network boot

Tabla 4.38 Configuración de la Dirección IP del Controlador RTC[117]

6. Presion el botón de **Reset** del controlador. El controlador se reinicia.

Nota: El controlador le toma 10 o 15 minutos reiniciar.

7. Quitar la conexión serial entre el Controlador y la PC.

4.8.2 Configuración del DHCP del Controlador de la Central Mitel

1. Una vez ingresada la clave del Controlador de la Central abrir el ***System Administration Tool.***
2. En la sección ***System Administration*****,** abrir la carpeta del ***DHCP***.
3. En la sub-sección ***DHCP Subnet***, ingrese el nombre de la subred, dirección IP y máscara.

[117] Tabla de Mitel Technician Handbook, Pág. 24.

4. En la sub-sección ***DHCP Static IP***, programe la dirección IP estática para el E2T, usando la información de la Tabla 4.39.

Programación de la Dirección Estática del E2T

Option ID	Valor	Notas / Ejemplos
Name	Nombre del E2T	
Subnet	Subred del E2T	Seleccionar una subred
IP Address	Dirección IP del E2T	162.168.1.5
Protocol	"BOOT o DHCP"	
Hardware Address		
Type	Dirección MAC	
Other - Type	n/a	Dirección IP del PC. Usado para actualizaciones de sofware
Address	Dirección MAC del Controlador (se encuentra atrás)	00:12:3a:4b:c5:67
Other - Address Length	n/a	
Client ID	n/a	

Tabla 4.39 Configuración de la Dirección Estática del E2T de la Central Mitel[118]

5. En la sub-sección ***DHCP IP Address Range***, programe el *scope* usando la información de la Tabla 4.40

Nota: Las siguientes direcciones IP (direcciones internas del controlador) son reservadas por los ASU's: 192.168.10.1 a 192.168.10.3; 192.168.11.1 a 192.168.11.3; 192.168.12.1 a 192.168.12.3; 192.168.13.1 a 192.168.13.3.

Programación del Rango de Direcciones IP (Scope)

Option ID	Valor	Notas / Ejemplos
Name of the range		
Subnet		Seleccionar una subred
IP Range Start	Inicio del Scope	162.168.1.15
IP Range End	Fin del Scope	162.168.1.25
Protocol	"BOOT or DHCP"	
Client's class ID must match name	Borrar la caja de selección	
Lease Time	2 Semanas	

Tabla 4.40 Configuración del Rango de Direcciones IP para un Scope[119]

[118] Tabla de Mitel Technician Handbook, Pág. 25
[119] Tabla de Mitel Technician Handbook, Pág. 26

Nota: En el DHCP IP Address Range si se elige como protocolo solo a BOOTP, no reconoce a los teléfonos ni a los PCs.

6. En la sub-sección **DHCP Options,** programar las opciones indicadas en la Tabla 4.41 , para el *scope* que se haya programado.

Opciones del DHCP Mitel

Option ID	Valor	Notas / Ejemplo
3	Dirección IP del Default Gateway (Router)	168.192.1.251
6	Dirección IP del servidor DNS	168.192.2.6
66	Servidor TFTP con formato ASCII String (tipicamente es el Controlador 3300 ICP)	168.192.1.2
67	TFTP BootFile (ASCII String = /sysro/e2t8260)	
128	Servidor TFTP con formato IP Address (tipicamente es el Controlador 3300 ICP)	168.192.1.2
129	RTC con formato IP Address (tipicamente es el Controlador 3300 ICP)	168.192.1.2
130	Servidor DHCP del teléfono IP (ASCII String = MITEL IP PHONE)	
132	VLAN ID para la VLAN de Voz (Hex - 32 bit word, or Numeric; opcional)	2
133	Prioridad, valores del 1 al 7 (Mitel recomienda 6, Numeric; opcional)	6

Tabla 4.41 Configuración de las Opciones del DHCP Mitel[120]

7. En la sub-sección **DHCP Server,** habilitar el DHCP interno del controlador.

Nota: El Real Time Complex (RTC) es usado para la señalización de los teléfonos IP y también el DHCP, TFTP, etc. El progreso de la llamada, el estatus del dispositivo y mensajes de actualización en la pantalla son enviados entre los teléfonos IP y el RTC. La tarjeta E2T (Ethernet to TDM) es donde la voz Ethernet se convierte a TDM y viceversa.

La configuración real del DHCP de la central Mitel para la red de Beaterio, se muestra en el Anexo 14.

[120] Tabla de Mitel Technician Handbook, Pág. 26

4.9 CONFIGURACIÓN DEL DHCP WINDOWS 2000 SERVER

El DHCP Windows 2000 Server, será el servidor que asignará dinámicamente las direcciones IP a todas las computadoras de la red de la Matriz, por lo tanto se deben crear diferentes *scopes* para cada una de la VLANs proyectadas para esta red.

La forma en que el Servidor DHCP diferencia cada una de las VLANs (o *scopes*) para asignarles sus respectivas direcciones IP es de acuerdo al *gateway* por el cual ingresan los DHCP *requests*, por lo tanto por cada *scope* existe un *gateway* diferente, que obviamente coincide con las direcciones IP asignadas a cada una de las VLANs en el switch multilayer (Cisco 4500).

Para crear y configurar un *scope* en el DHCP Windows 2000 server se realiza lo siguiente:

Se presiona el boton derecho del raton sobre el nombre del servidor (**pcored.petrocomercial.com)** y se elige la opción **New Scope…,** como se muestra en la Figura 4.2.

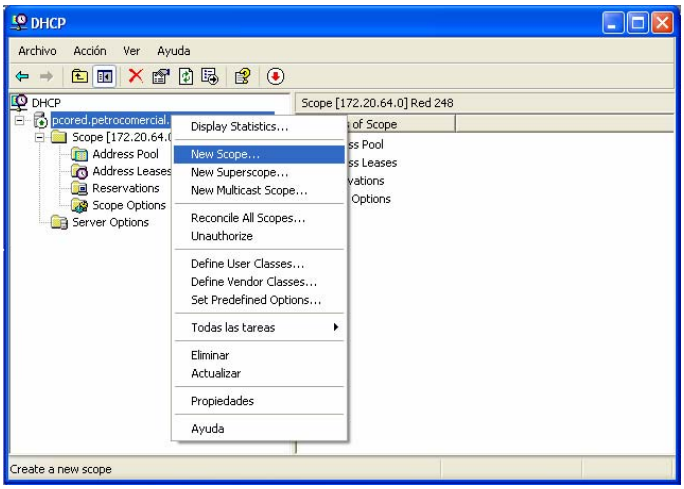


Figura 4.2 Creación de un Nuevo Scope

Luego simplemente se completan cada uno de los parámetros que se soliciten a lo largo de las ventanas, como se muestra a continuación:

Se ingresa el nombre y descripción del Nuevo *Scope*:

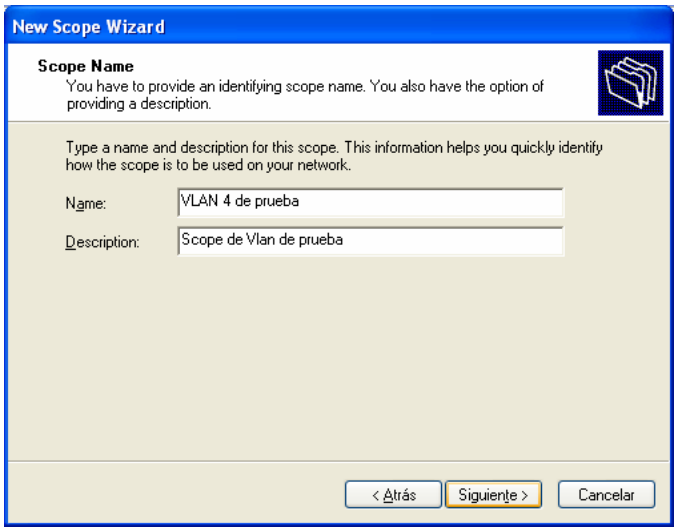


Figura 4.3 Nombre y Descripción del Scope

Se ingresa el rango de direcciones IP, la dirección IP inicial y la final, y la máscara de red a la cual pertenece el *scope* (o VLAN).

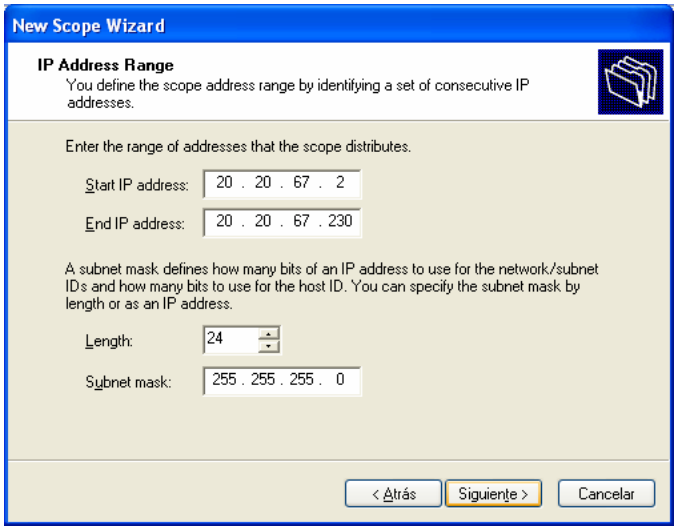


Figura 4.4 Configuración del Rango de Direcciones IP para un Scope

A continuación aparece otra ventana para añadir exclusiones, es decir direcciones o rango de direcciones, que no son distribuidas por el servidor, en nuestro caso no lo utilizamos. Luego, en la siguiente ventana, se especifica el tiempo de arriendo del cliente, es decir el tiempo que puede tener un cliente la dirección IP dentro del *scope*.

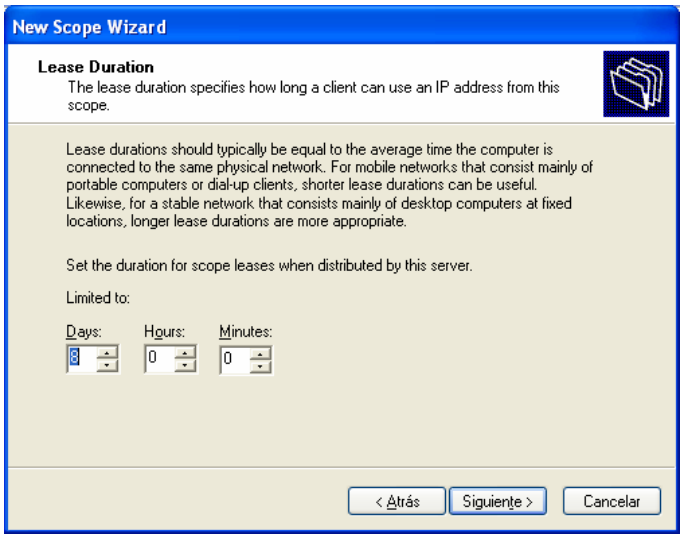


Figura 4.5 Configuración del Tiempo de Arrendamiento de Direcciones

La siguiente ventana le pregunta si desea configurar las opciones del servidor DHCP, y se responde que sí desea hacerlo. A continuación, se ingresa el *default gateway* respectivo para el *scope*, o lo que es lo mismo la dirección IP de la VLAN asignada en el switch multilayer Cisco 4500.

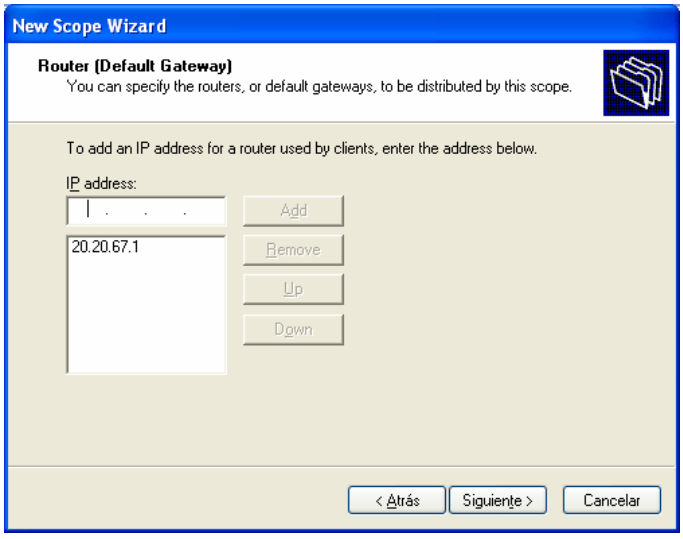


Figura 4.6 Configuración de la Dirección IP del Gateway del Scope

Se ingresa el Nombre del dominio de Petrocomercial, y el nombre y dirección IP del servidor DNS de la red, de acuerdo al nuevo direccionamiento ya establecido.

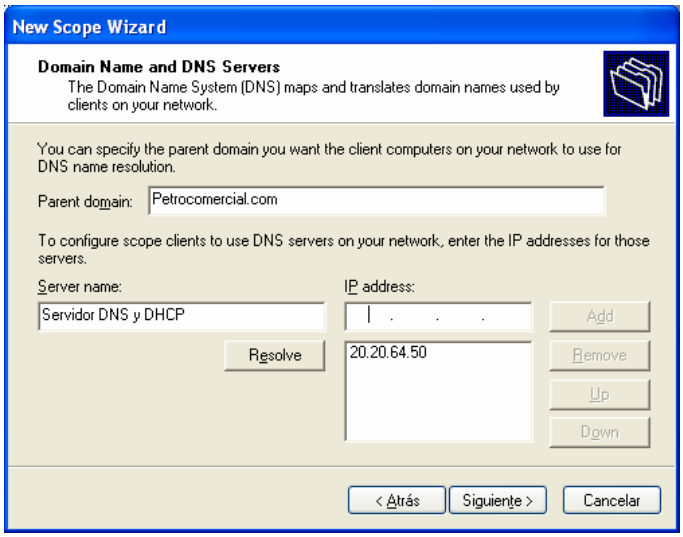


Figura 4.7 Configuración del Nombre de Dominio y Dirección IP del DNS

Después, en otra ventana se puede configurar el nombre y dirección IP de Servidores WINS, pero debido a que actualmente no se cuenta con ninguno, simplemente se pasa a la siguiente ventana.

Y finalmente en otra ventana, le pregunta si desea activar el *scope* en ese momento, o luego, para que los clientes empiecen a tomar las direcciones arrendadas. Como se muestra en la Figura 4.8.

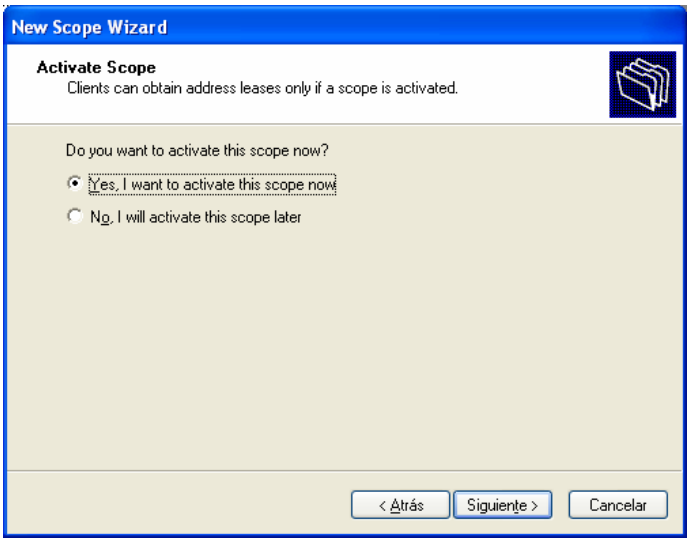


Figura 4.8 Confirmación de la creación del Scope

Además, en este DHCP, existe la opción de crear direcciones reservadas, es decir asignar siempre la misma dirección IP al mismo cliente.

4.10 ESCENARIOS COMUNES DE CONFIGURACIÓN

El escenario 1, es uno de los más comunes en las redes de Petrocomercial, donde encontramos una computadora detrás de un teléfono, y éste último conectado a su vez a un puerto de un switch. Este puerto debe ser un puerto troncal para que soporte tanto la VLAN de voz como la VLAN de datos (VLAN nativa). El protocolo de encapsulación seteado en la troncal necesariamente es el 802.1Q, debido a que se está conectando un equipo Cisco con un equipo Mitel. El puerto al cual se conecta el Controlador de la Central Mitel (DHCP), debe ser un puerto de acceso a la VLAN de voz.

Dependiendo del usuario o departamento al cual pertenece la computadora y de acuerdo al diseño de VLANs ya establecido, se determina que VLAN será la nativa en el puerto troncal.

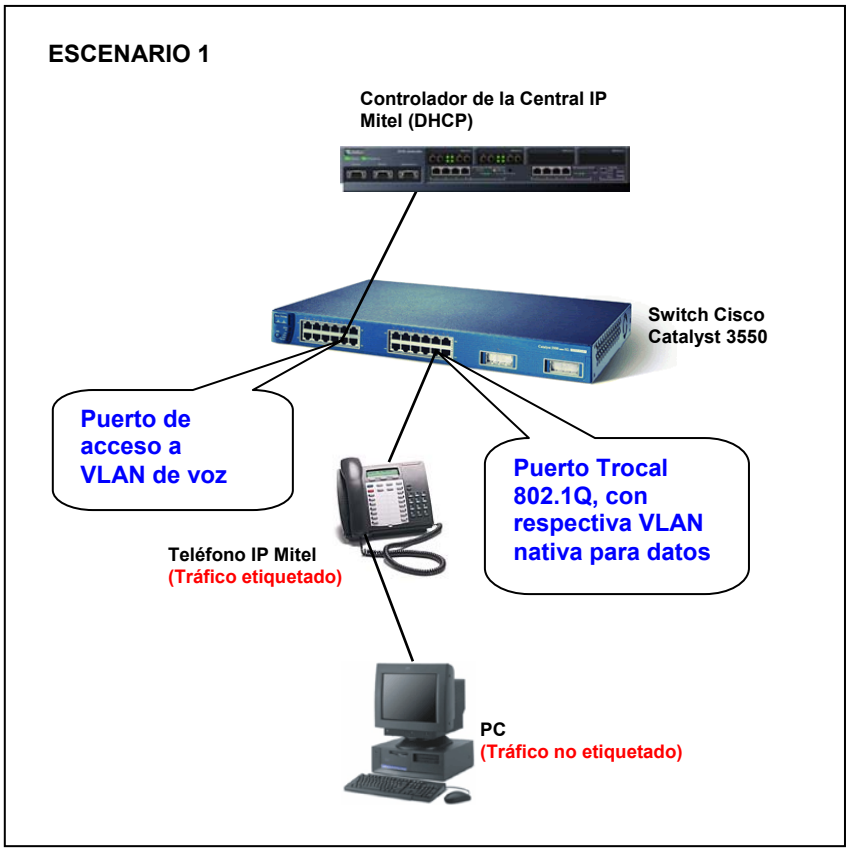


Figura 4.9 Escenario de Configuración 1

El escenario 2, solo comprende de un teléfono IP y obviamente el controlador de la central. El puerto al cual se conecta el teléfono IP puede ser un puerto de acceso a la

VLAN de voz, aunque se aconseja que este puerto sea troncal, para conectar sin problemas una computadora al teléfono; obviamente configurando la respectiva VLAN nativa de datos de acuerdo a quién utiliza el teléfono.

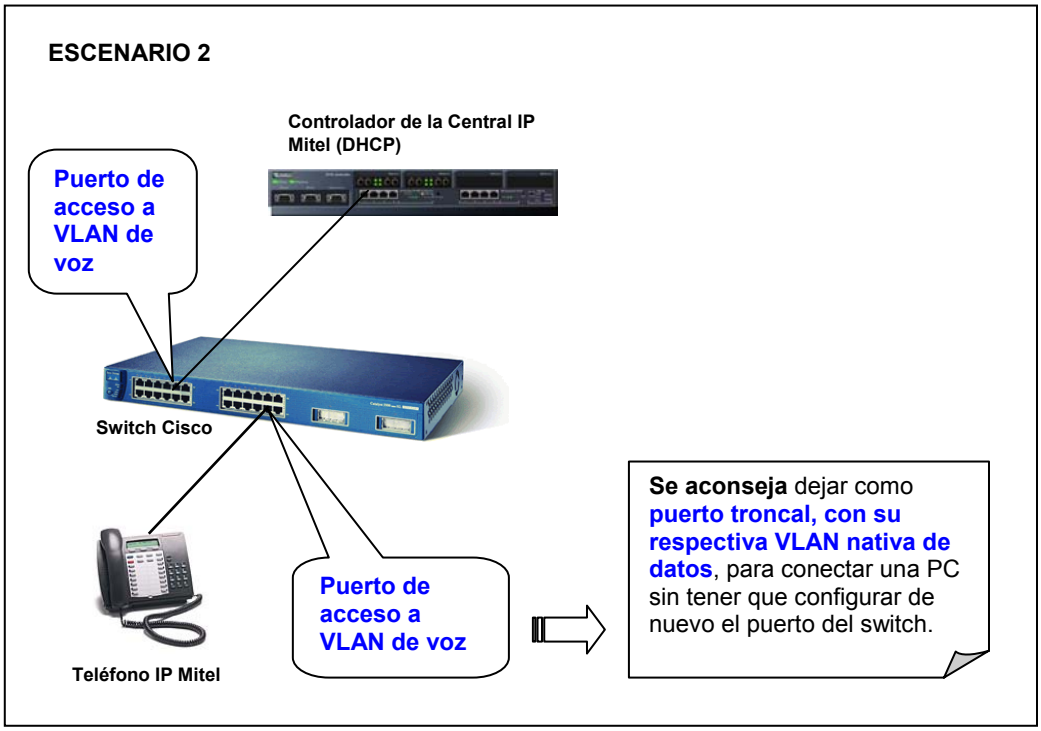


Figura 4.10 Escenario de Configuración 2

El tercer escenario lo comprende solo de una computadora conectada a un puerto de un switch, puerto que será configurado como puerto de acceso a la respectiva VLAN de datos, aunque también se aconseja setear este puerto como troncal, para evitar problemas en el caso de poner un teléfono IP entre la computadora y el switch.

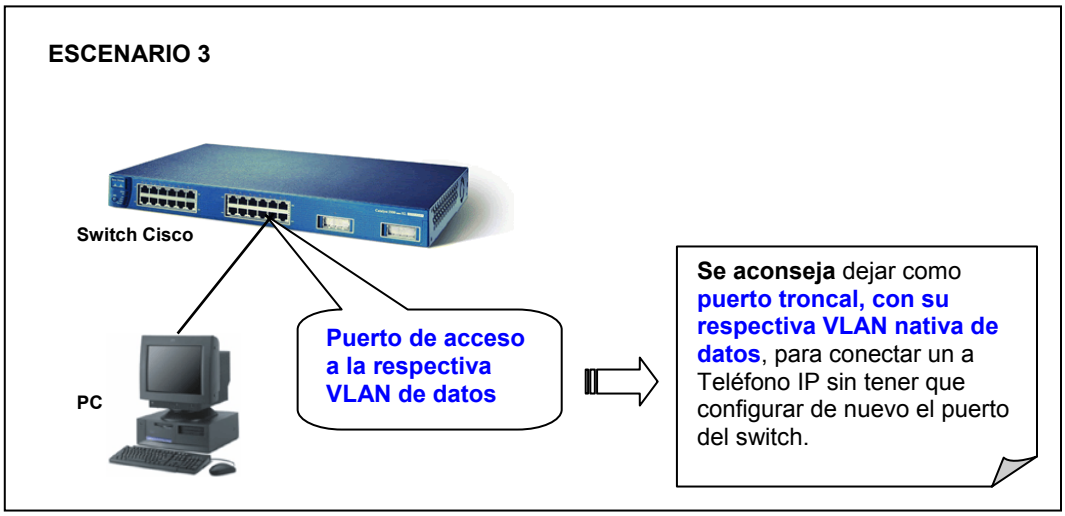


Figura 4.11 Escenario de Configuración 3

Con el último escenario se debe tener mucho cuidado porque incluye un switch no inteligente, tales como los switches Dlink, 3COM o Cnet de 6 u 8 puertos, que no analizan los campos de VLAN ID y Prioridad, y simplemente transmiten los paquetes. Por lo tanto todas las computadoras conectadas a este switch no inteligente pertenecerán a la misma VLAN, que es la VLAN nativa del puerto troncal con el cual se conecta este switch. Por lo demás, este escenario, tiene el mismo comportamiento que el escenario 1.

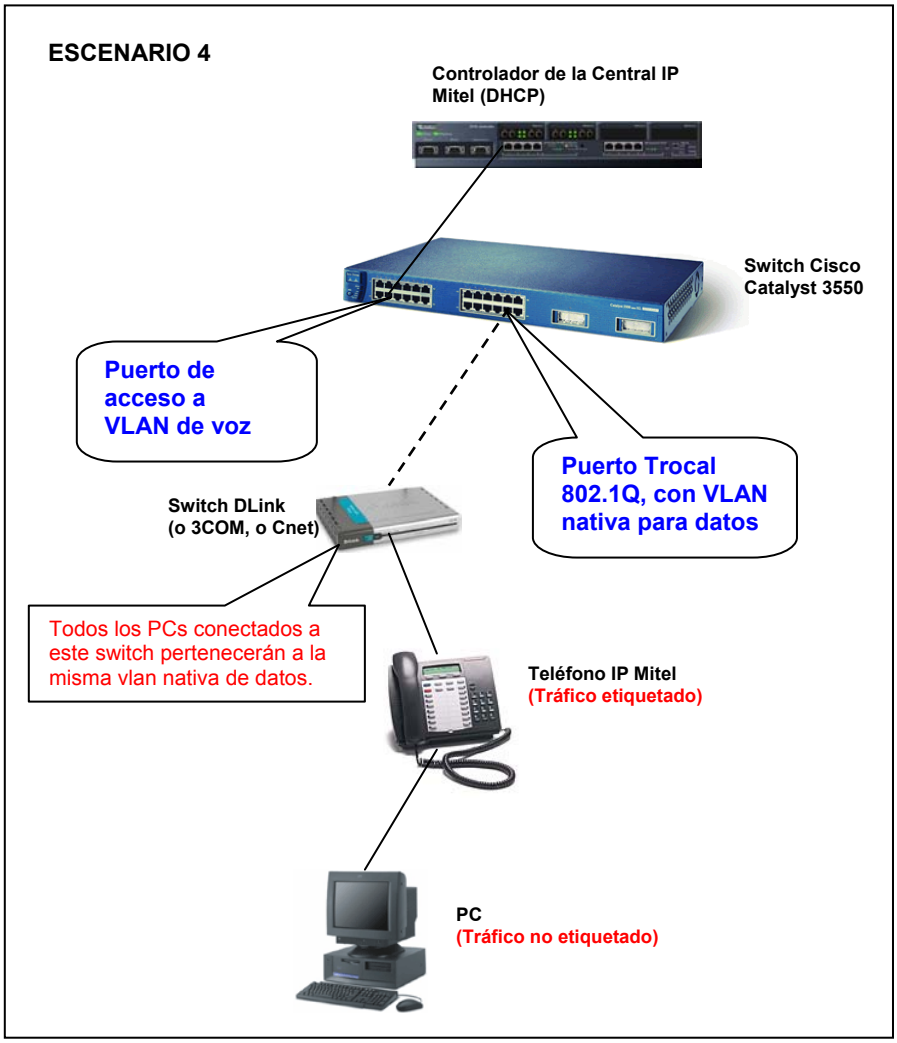


Figura 4.12 Escenario de Configuración 3

4.11 CONFIGURACION DE LA RED DE LA MATRIZ

En el **switch multilayer Cisco Catalyst 4507R** se debe configurar lo siguiente:

- Crear las VLANs:
  - VLAN 1 – *Default* (Gestión de Red)
  - VLAN 2 – Gestión de Servidores
  - VLAN 3 – Voz
  - VLAN 4 – Administrativa
  - VLAN 5 – Comercialización
  - VLAN 6 – General
  - VLAN 7 – Filiales
  - VLAN 8 – Extranet (Internet)

- Configurar como puertos troncales a las interfaces que van hacia los otros switches, con encapsulación 802.1Q y VLAN nativa 1.

- Configurar enrutamiento
  - Habilitar enrutamiento en el switch.
  - Crear interfaces virtuales de switch (SVIs) o interfaces de capa 3, para las seis primeras VLANs con las respectivas direcciones IP ya establecidas, es decir la VLAN 7 y la VLAN 8 no tienen enrutamiento directo con el resto de las VLANs, porque estas deben enrutarse primero a las interfaces del Firewall, para que este realice el filtrado de tráfico que sea necesario. Esto se debe a que estas VLANs constituyen los accesos a redes externas para la red de Petrocomercial.
  - Configurar los puertos que se conectan a los diferentes routers de acceso como puertos enrutados, con su respectiva dirección IP.
  - Habilitar RIP versión 2
  - Configurar las respectivas direcciones de red de cada VLAN (1 – 6) o la dirección de red que contiene a esas VLANs, en el protocolo de enrutamiento RIP.
  - Crear una ruta estática por defecto a la dirección de la WAN.
  - Configurar las rutas estáticas necesarias para tener comunicación con los routers (y firewall) que ofrecen los diferentes accesos.

  - Enrutar los pedidos DHCP de las VLANs 1,2,4,5 y 6 a la dirección de la central o servidor DHCP en la VLAN 3.

- Configurar VTP
  - Crear el dominio VTP Matriz
  - Habilitar la versión 2 de VTP
  - Habilitar el modo Servidor VTP
  - Habilitar VTP *Pruning* (Solo en el servidor)

- Configurar los puertos del switch de acuerdo a los escenarios ya descritos.
  - Configurar los puertos que se conectan a un solo teléfono IP, a una sola computadora o a un teléfono IP con computadora, como puertos troncales, con encapsulación 802.1Q y con su respectiva VLAN nativa para datos de acuerdo al usuario o departamento.
  - Configurar como puerto troncal al puerto que se conecta a un switch no inteligente, con la respectiva VLAN nativa de datos que van a utilizar todos las computadoras que se conecten a ese switch.
  - El puerto al cual se conecta la central Mitel es un puerto de acceso a su respectiva VLAN.

- Configurar STP
  - Habilitar el modo PVST+, aunque por defecto ya está habilitado este modo.
  - Asignar una prioridad baja en todas las VLANs de este switch, para que sea el *root switch* de cada una de las topologías *Spanning-Tree* de las VLANs.
  - Dejar habilitado STP en los puertos que vayan hacia otros switches y los que están sin conexión.
  - Deshabilitar STP en los puertos que se conectan a un solo teléfono IP, a una sola computadora o a un teléfono IP con computadora. Y también deshabilitar STP al puerto que se conecta a la central IP Mitel.

- Configurar QoS
  - Habilitar QoS en el switch
  - Aceptar la prioridad recibida en los puertos donde se conecten teléfonos IP.

En los **otros switches Cisco de la Matriz** se debe configurar lo siguiente:

- Configurar como puertos troncales a las interfaces que van hacia los otros switches, con encapsulación 802.1Q y VLAN nativa 1.

- Configurar como *gateway* la dirección IP de la VLAN 1 definida en el switch multilayer Cisco Catalyst 4507R.

- Configurar VTP
    - Crear el dominio VTP Matriz
    - Habilitar la versión 2 de VTP
    - Habilitar el modo cliente VTP

- Configurar STP
    - Habilitar el modo PVST+, aunque por defecto ya está habilitado este modo.
    - Dejar habilitado STP en los puertos que vayan hacia otros switches y los que están sin conexión.
    - Deshabilitar STP en los puertos que se conectan a un solo teléfono IP, a una sola computadora o a un teléfono IP con computadora.

- Configurar QoS
    - Habilitar QoS en los switches Cisco 3550 (en los switches 3500 XL no es necesario).
    - Aceptar la prioridad recibida en los puertos donde se conecten teléfonos IP, en los swtiches Cisco 3550 (en los switches 3500 XL no es necesario).

En el **router Vanguard Motorota** 6455 se debe configurar lo siguiente:

- Cambiar la dirección IP y máscara de la interfaz LAN del router, de acuerdo al direccionamiento establecido.

- Habilitar RIP versión 2 en la interfaz LAN del router

- Dejar el VLAN ID de la interfaz LAN en 1.

- No configurar ningún tipo de encapsulación

- Cambiar las rutas estáticas que apuntan a los distintos routers (y firewall), con un valor de *next hop* igual a la dirección de la interfaz del switch Cisco 4500 con la cual se conecta el router Vanguard.

En los **routers IBM y Cisco que proveen los diferentes accesos** se debe configurar lo siguiente:

- Cambiar la dirección IP y máscara de la interfaz LAN del router, de acuerdo a la nueva disposición de direcciones.

- Cambiar la dirección IP del próximo salto de la ruta estática que apunta a la red interna de Petrocomercial, de acuerdo a la interfaz del switch 4507R a la cual está conectado el router.

En el **controlador de la central IP Mitel** se debe configurar lo siguiente:

- Configurar la dirección IP, máscara y *gateway* del controlador de la central, de acuerdo al nuevo direccionamiento.

- Configurar el DHCP del controlador de la central IP Mitel para los teléfonos IP.
    - Crear una subred por cada VLAN, ingresando el nombre de la subred, la dirección IP de la subred y la máscara.
    - Configurar la dirección IP, dirección MAC y la subred de la VLAN de voz del E2T de la Central Mitel.
        - Crear el rango de direcciones IP para la subred de la VLAN de voz, de acuerdo al nuevo direccionamiento, y para el resto de subredes, que corresponden al tráfico de datos, utilizar las misma direcciones ya establecidas o configurar rangos ficticios de direcciones IP, porque al fin y al cabo estas direcciones las va a desechar el teléfono

IP cuando las reciba en la respuesta del primer *request* DHCP. Además configurar el tiempo de arriendo de estas direcciones.

- Configurar las opciones del DHCP
  - Las siguientes opciones deben ser aplicadas al *scope* de la VLAN de Voz:
    - Dirección IP del servidor DNS que se encuentra en la Matriz.
    - El nombre del servidor TFTP, la dirección IP del servidor TFTP y la dirección IP del RTC, que todos ellos con sus respectivos formatos, corresponden a la dirección IP de la Central Mitel.
    - El nombre del TFTP Boot File.
    - El nombre del servidor del teléfono IP, MITEL IP PHONE.
  - Para cada subred (VLAN) se aplican las siguientes opciones:
    - El *gateway* respectivo de la VLAN.
    - El VLAN ID de la VLAN de Voz, (3).
    - La prioridad de la VLAN de Voz, (6).

    Nota: En el *scope* de la VLAN de Voz no se configuran los parámetros VLAN ID y Prioridad.

En el **DHCP Windows 2000 Server** se debe configurar lo siguiente:

- Primeramente este servidor debe estar con la nueva dirección IP, máscara y *gateway*, ya establecidos en el nuevo direccionamiento.

- Crear un *Scope* para cada VLAN (1 -6) de la siguiente forma:

  - Asignar el Nombre del *Scope* y la descripción.
  - Asignar un rango de direcciones para las computadoras de esa VLAN y su la respectiva mascara de la subred a la cual pertenecen.
  - Configurar un tiempo de arriendo para las direcciones que se asignan a las computadoras.

- Configurar el *gateway* por el cual ingresan los *request* de estos hosts, es decir es la dirección IP de la VLAN, configurada en el switch multilayer Cisco Catalyst 4507R.
- Configurar el nombre del dominio, que es Petrocomercial.com y la dirección del Servidor DNS, que en este caso es la misma dirección del DHCP.

Si se desea conocer la configuración del diseño de VLANs planteado por la Propuesta 1, recurrir al Anexo 10.

En la Figura 4.13 se muestra el resumen de la configuración principal de los equipos de la Matriz, utilizando la propuesta 2 del diseño de VLANs.

En la Figura 4.14 se detalla la configuración de los puertos de los switches de acuerdo a que dispositivos se encuentran conectados; además de la configuración básica de los switches Cisco 3500 XL y 3550 que funcionan en la capa de acceso (según el Modelo Jerárquico Cisco).

En la Figura 4.15 se muestra el mapa lógico de capa 3 para la red de la Matriz, detallando las rutas estáticas de capa uno de los equipos, las direcciones IP de las interfaces, la definición de interfaces virtuales, en reenvío de tráfico (DHCP) hacia los respectivos servidores y la configuración de enrutamiento dinámico en los respectivos dispositivos. Para construir adecuadamente este mapa de rutas se tomo como apoyo obviamente las rutas actuales, como se pueden observar en el Anexo 13.

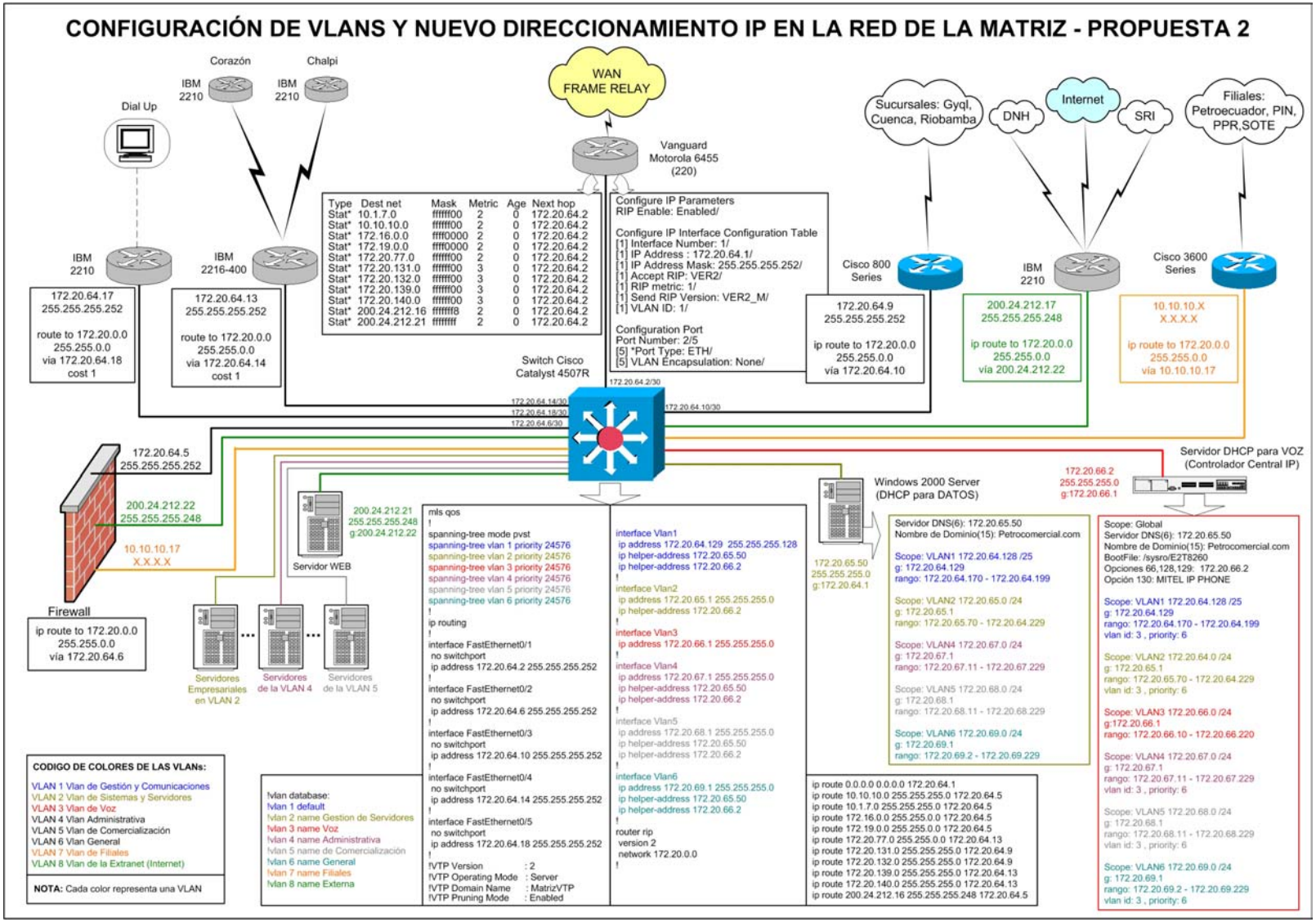


Figura 4.13 Configuración de VLANs y Direccionamiento IP en la Red de la Matriz

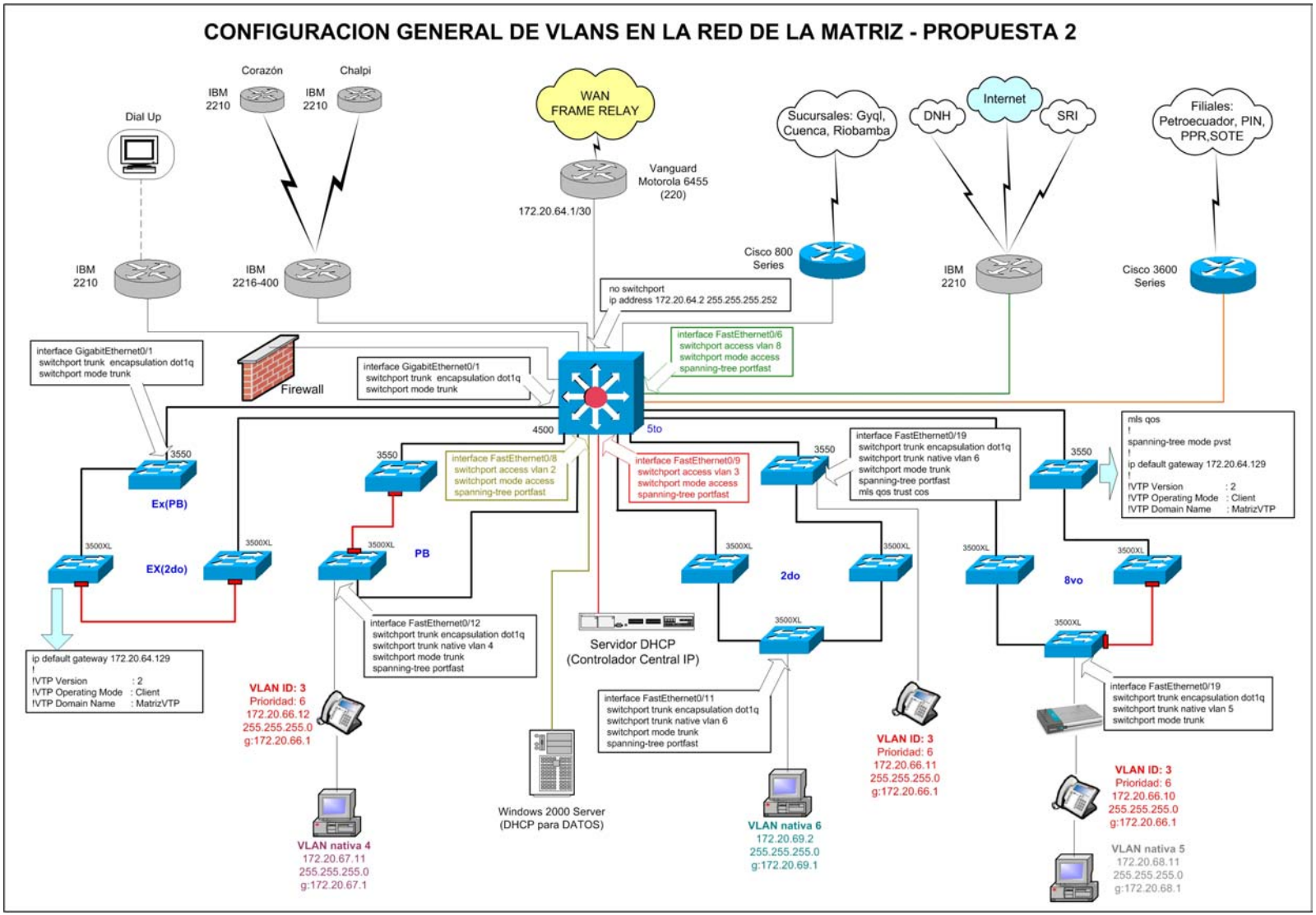


Figura 4.14 Configuración General de VLANs en la Red de la Matriz

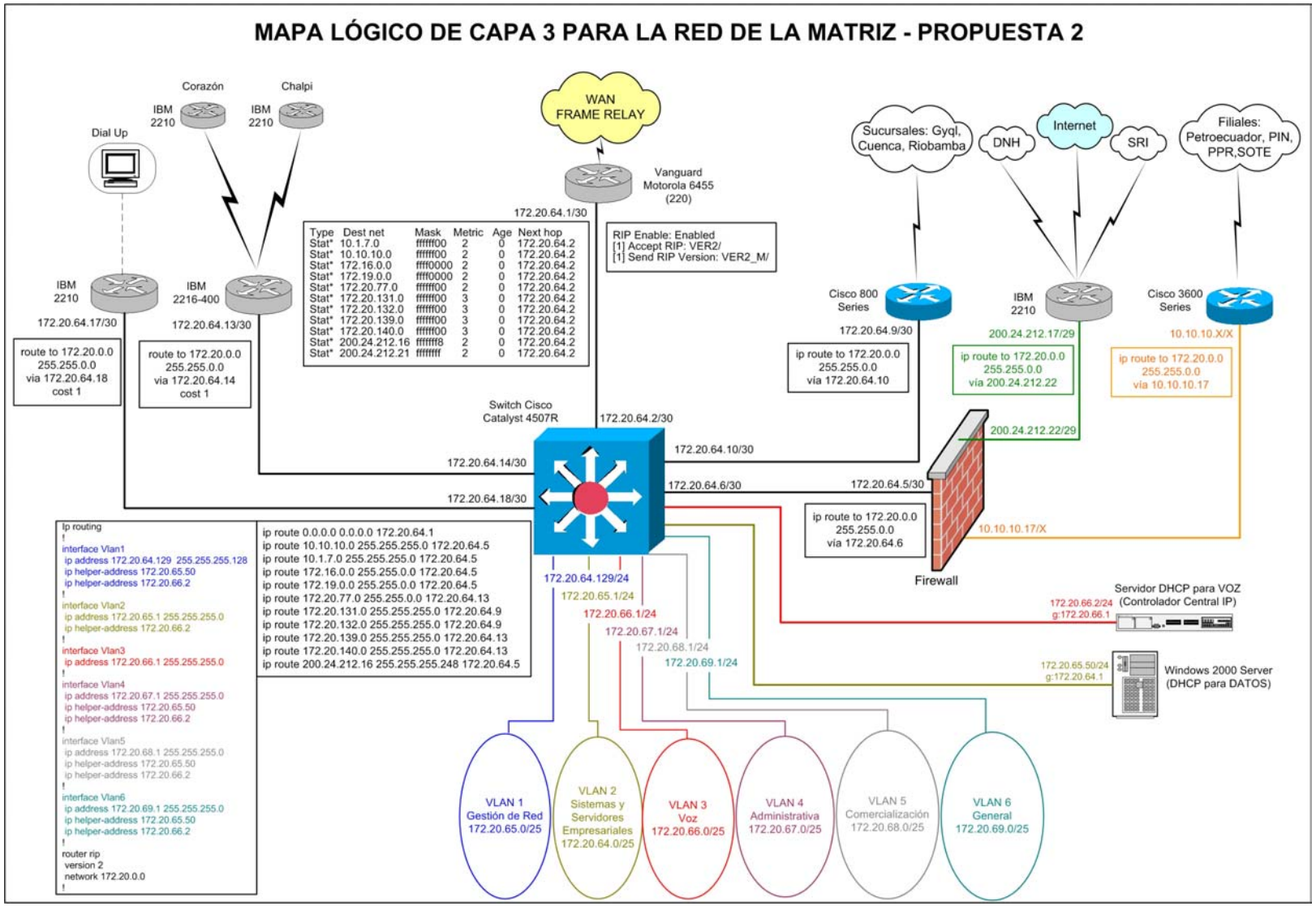


Figura 4.15 Mapa Lógico de Capa 3 para la Red de la Matriz

4.12 CONFIGURACION DE LA RED DE BEATERIO

En el **switch multilayer Cisco Catalyst 3550 de Telecomunicaciones** se debe configurar lo siguiente:

- Crear las VLANs:
  - VLAN 1 – *Default* (VLAN de Gestión)
  - VLAN 2 – Automatización
  - VLAN 3 – Voz
  - VLAN 4 – Datos

- Configurar como puertos troncales a las interfaces que van hacia los otros switches, con encapsulación 802.1Q y VLAN nativa 1.

- Configurar enrutamiento
  - Habilitar enrutamiento en el switch.
  - Crear SVIs para todas las VLANs, y asignarles una dirección IP a cada una.
  - Configurar el puerto que se conecta al router Vanguard Motorota 6455 (220) como puerto enrutado, con su respectiva dirección IP.
  - Habilitar RIP versión 2
  - Configurar las direcciones de red de cada VLAN o dirección de red que contiene a esas VLANs, en el protocolo de enrutamiento RIP.
  - Crear una ruta estática por defecto a la dirección de la interfaz LAN del router Vanguard que tiene acceso directo a la WAN.
  - Enrutar los pedidos DHCP de las VLANs 1,2 y 4 a la dirección de la central o servidor DHCP en la VLAN 3.

- Configurar VTP
  - Crear el dominio VTP Beaterio
  - Habilitar la versión 2 de VTP
  - Habilitar el modo Servidor VTP
  - Habilitar VTP *Pruning* (Solo en el servidor)

- Configurar los puertos del switch de acuerdo a los escenarios ya descritos.
    - Configurar los puertos que se conectan a un solo teléfono IP, a una sola computadora o a un teléfono IP con computadora, como puertos troncales, con encapsulación 802.1Q y con su respectiva VLAN nativa para datos de acuerdo al usuario o departamento.
    - Configurar como puerto troncal al puerto que se conecta a un switch no inteligente, con la respectiva VLAN nativa de datos que van a utilizar todos las computadoras que se conecten a ese switch.
    - El puerto al cual se conecta la central Mitel es un puerto de acceso a su respectiva VLAN.

- Configurar STP
    - Habilitar el modo PVST+, aunque por defecto ya está habilitado este modo.
    - Asignar una prioridad baja en todas las VLANs de este switch, para que sea el *root switch* de cada una de las topologías *Spanning-Tree* de las VLANs.
    - Dejar habilitado STP en los puertos que vayan hacia otros switches y los que están sin conexión.
    - Deshabilitar STP en los puertos que se conectan a un solo teléfono IP, a una sola computadora o a un teléfono IP con computadora. Y también deshabilitar STP al puerto que se conecta a la central IP Mitel.

- Configurar QoS
    - Habilitar QoS en el switch
    - Aceptar la prioridad recibida en los puertos donde se conecten teléfonos IP.

En los **otros switches Cisco de Beaterio** se debe configurar lo siguiente:

- Configurar como puertos troncales a las interfaces que van hacia los otros switches, con encapsulación 802.1Q y VLAN nativa 1.

- Configurar como *gateway* la dirección IP de la VLAN 1 definida en el switch multilayer Cisco Catalyst 3550 (de Telecomunicaciones).

- Configurar VTP
    - Crear el dominio VTP Beaterio
    - Habilitar la versión 2 de VTP
    - Habilitar el modo cliente VTP

- Configurar los puertos del switch de acuerdo a los escenarios ya descritos.
    - Configurar los puertos que se conectan a una computadora, a un teléfono, o a un teléfono con computadora, como puertos troncales, con encapsulación 802.1Q y con su respectiva VLAN nativa para datos de acuerdo al usuario o departamento.
    - Los puertos a los cuales se conectan el router Vanguard y la central Mitel son puertos de acceso a su respectiva VLAN.

- Configurar STP
    - Habilitar el modo PVST+ en los switches que sea posible, aunque por defecto ya viene configurado este modo, en todos los switches que se están utilizando.
    - Dejar habilitado STP en los puertos que vayan hacia otros switches y los que están sin conexión.
    - Deshabilitar STP en los puertos que se conectan a un solo teléfono IP, a una sola computadora o a un teléfono IP con computadora. Y también deshabilitar STP en los puertos a los que se conectan el router Vanguard y la central Mitel.

- Configurar QoS
    - Habilitar QoS en el otro switch Cisco 3550 (en éste puede habilitarse).
    - Aceptar la prioridad recibida en los puertos donde se conecten teléfonos IP, en el otro swtich Cisco 3550, que estará en Jefatura, (solo éste switch acepta esta configuración).

En el **router Vanguard Motorota** 6455 se debe configurar lo siguiente:

- Cambiar la dirección IP y máscara de la interfaz LAN del router, de acuerdo al direccionamiento establecido.

- Habilitar RIP versión 2 en la interfaz LAN del router

- Dejar el VLAN ID de la interfaz LAN en 1.

- No configurar ningún tipo de encapsulación.

En el **controlador de la central IP Mitel** se debe configurar lo siguiente:

- Configurar la dirección IP, máscara y *gateway* del controlador de la central, de acuerdo al nuevo direccionamiento.

- Configurar el DHCP del controlador de la central IP Mitel para los teléfonos IP y para las computadoras.
    - Crear una subred por cada VLAN, ingresando el nombre de la subred, la dirección IP de la subred y la máscara.
    - Configurar la dirección IP, dirección MAC y la subred de la VLAN de voz del E2T de la Central Mitel.
    - Crear un rango de direcciones IP por cada subred y configurar el tiempo de arriendo de estas direcciones, que corresponden a los rangos de:
        - Las computadoras de Telecomunicaciones en VLAN 1.
        - Las computadoras o equipos para Automatización en VLAN 2.
        - Los teléfonos IP en VLAN 3.
        - Las computadoras de Beaterio (excepto de Telecomunicaciones y Automatización) en VLAN 4.
    - Configurar las opciones del DHCP
        - Las siguientes opciones deben ser aplicadas en forma Global (*Scope*), para que les afecte a todos los *scopes*:
            - Dirección IP del servidor DNS que se encuentra en la Matriz.
            - El nombre del servidor TFTP, la dirección IP del servidor TFTP y la dirección IP del RTC, que todos ellos con sus respectivos formatos, corresponden a la dirección IP de la Central Mitel.
            - El nombre del TFTP Boot File.

- El nombre del teléfono IP, MITEL IP PHONE.

- Para cada subred (VLAN) se aplican las siguientes opciones:
  - El *gateway* respectivo de la VLAN.
  - El VLAN ID de la VLAN de Voz (3)
  - La prioridad de la VLAN de Voz. (6)

  Nota: En el *scope* de la VLAN de Voz no se configuran los parámetros VLAN ID y Prioridad.

Si se desea conocer la configuración del diseño de VLANs planteado por la Propuesta 1, recurrir al Anexo 12.

El detalle de la asignación de VLANs a los puertos de los switches, que actualmente están en funcionamiento en Beaterio se muestra en el Anexo 15, y la configuración real de los equipos de Beaterio e información que corrobora el funcionamiento adecuado de esta implementación, está en el Anexo 16.

En la Figura 4.16 se muestra el resumen de la configuración principal de todos los equipos de Beaterio, incluyendo la configuración de los puertos de los switches de acuerdo a que dispositivos se encuentran conectados, según la segunda propuesta del diseño de VLANs.

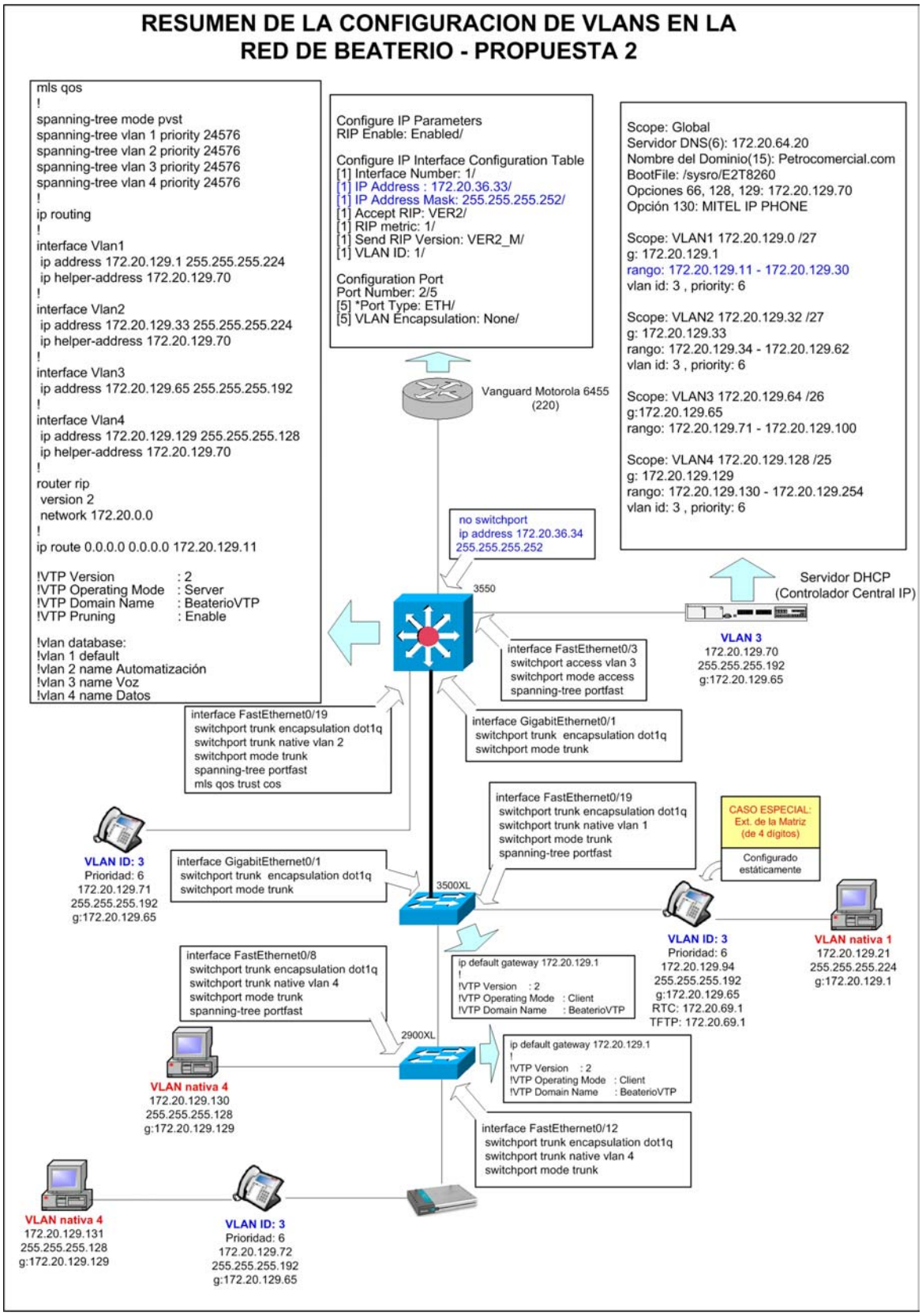


Figura 4.16 Resumen de la Configuración de VLANs en la Red de Beaterio

CAPITULO V

PRUEBAS

5.1 PRUEBAS EN LA RED DE BEATERIO

Todas las pruebas que se detallan a continuación, fueron realizadas en la red del Beaterio. Gracias a estas pruebas y a la configuración realizada en esta red (Ver Anexo, este proyecto ratifica que las configuraciones expuestas en el Capítulo tres, son propuestas de configuración con fundamentos reales. Además se debe tomar en cuenta que tanto la red de Beaterio como la Matriz tienen propuestas de diseño similares y los principales equipos a configurar son los mismos o tienen las mismas características de configuración como son el switch 3550 y el switch 4500.

5.1.1 Comportamiento de los hosts con el DHCP de la Central Mitel

A continuación se realizará un análisis completo del Comportamiento del DHCP del Controlador de la Central con los teléfonos IP que están conectados a una PC:

Se comprobó que efectivamente el teléfono IP si realiza dos DHCP requests. El teléfono realiza el primer DHCP request sobre la VLAN nativa, porque obviamente no sabe todavía a que VLAN pertenece. Y la respuesta a este request también la recibe sobre esta misma VLAN.

En la respuesta del primer DHCP request toma el VLAN ID y la prioridad que le envía el DHCP. Pero descarta la dirección IP que le haya enviado.

Nota: El scope que utiliza el DHCP en el primer request (que es el scope de la VLAN nativa de los puertos troncales), necesariamente debe tener configurado un rango de direcciones IP, aunque sea para que el teléfono IP descarte la dirección que elija de este rango. Acotación que se debe tomar en cuenta especialmente en la configuración del DHCP de la central de la Matriz, porque en el caso del DHCP de la central de Beaterio, estos rangos inevitablemente deben existir para asignar estas direcciones IP a las computadoras.

Por lo tanto el segundo DHCP request ya lo realiza sobre la VLAN de voz, que corresponde al VLAN ID recibido.

De la respuesta del segundo DHCP request, no toma en cuenta el nuevo VLAN ID ni prioridad enviados, (porque debería rechazar la conexión si estos parámetros son diferentes en las dos respuestas de los requests, y no lo hace). Lo que si acepta del segundo DHCP request es la nueva dirección IP enviada.

Nota: Si en el servidor DHCP, se han activado las opciones 132 VLAN ID y 133 Prioridad para el scope de los teléfonos IP (VLAN de voz), entonces todo puerto del switch, ya sea solo conectado a un teléfono IP, o a un teléfono IP con PC; deben ser puertos troncales; porque si estos puertos son de acceso, simplemente el teléfono no recibe la dirección IP y no se activa el teléfono.

Por lo tanto, para evitar este tipo de problemas y conociendo que de la respuesta del segundo DHCP request no se toman en cuenta: el VLAN ID ni Prioridad, entonces no se configurarán estos dos parámetros en el Scope de téfonos IP o VLAN de voz. Creando también así la posibilidad de conectar un solo teléfono IP (sin PC) a un puerto de acceso del switch.

Gracias a las opciones que ofrece el Servidor DHCP de la central Mitel, éste puede manejar varios grupos de teléfonos en diferentes VLANs, o mejor dicho varios scopes de direcciones IP en diferentes VLANs. Esto lo consigue utilizando un gateway por cada VLAN o rango de direcciones; es decir el Servidor DHCP para saber de que scope tomar la dirección IP, antes verifica porque gateway ingresó el DHCP request.

En conclusión el comportamiento de los teléfonos IP con el servidor DHCP se resume de la siguiente manera: El teléfono IP de la respuesta del primer request toma el VLAN ID y la Prioridad, mientras que de la respuesta del segundo request solo toma la dirección IP.

Aprovechando éste comportamiento de los teléfonos IP y que las computadoras toman directamente de la respuesta del primer request la dirección IP y descartan los valores de VLAN ID y Prioridad enviados por el Servidor DHCP; se puede utilizar el mismo Servidor DHCP para las computadoras.

Realmente no es conveniente tener un solo DHCP para los teléfonos y computadoras, pero debido a que la cantidad de computadoras y teléfonos IP en la Red de Beaterio no es muy grande, esta opción es válida, y más aun sabiendo utilizar adecuadamente el comando ip helper-address del switch de capa 3 para que enrute los pedidos broadcast de DHCP a la VLAN donde se encuentra el Servidor DHCP, y manipulando bien las opciones de VLAN ID y Prioridad para cada uno de los scopes (o VLANs) en el Servidor DHCP.

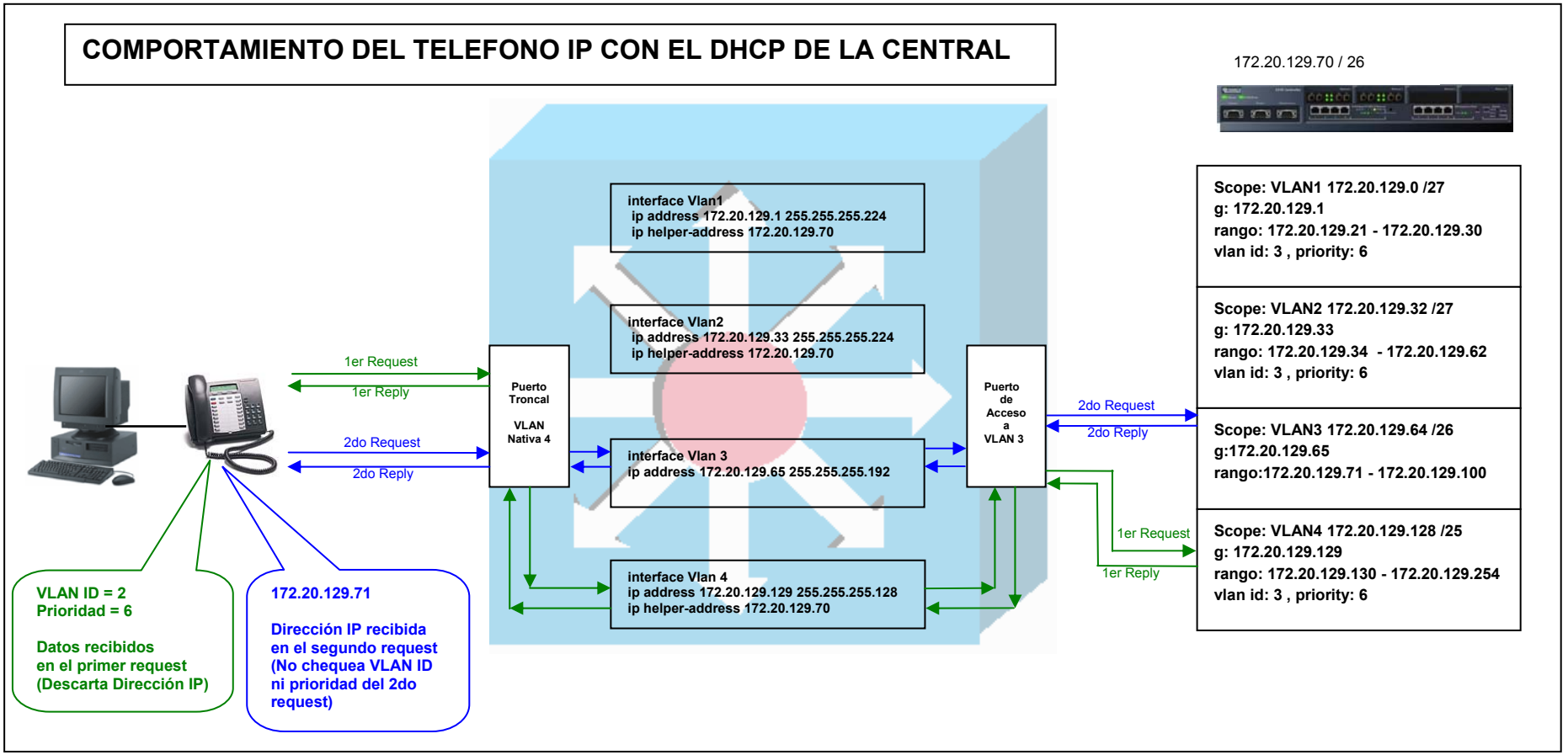


Figura 5.1 Comportamiento del Teléfono IP con el DHCP Mitel

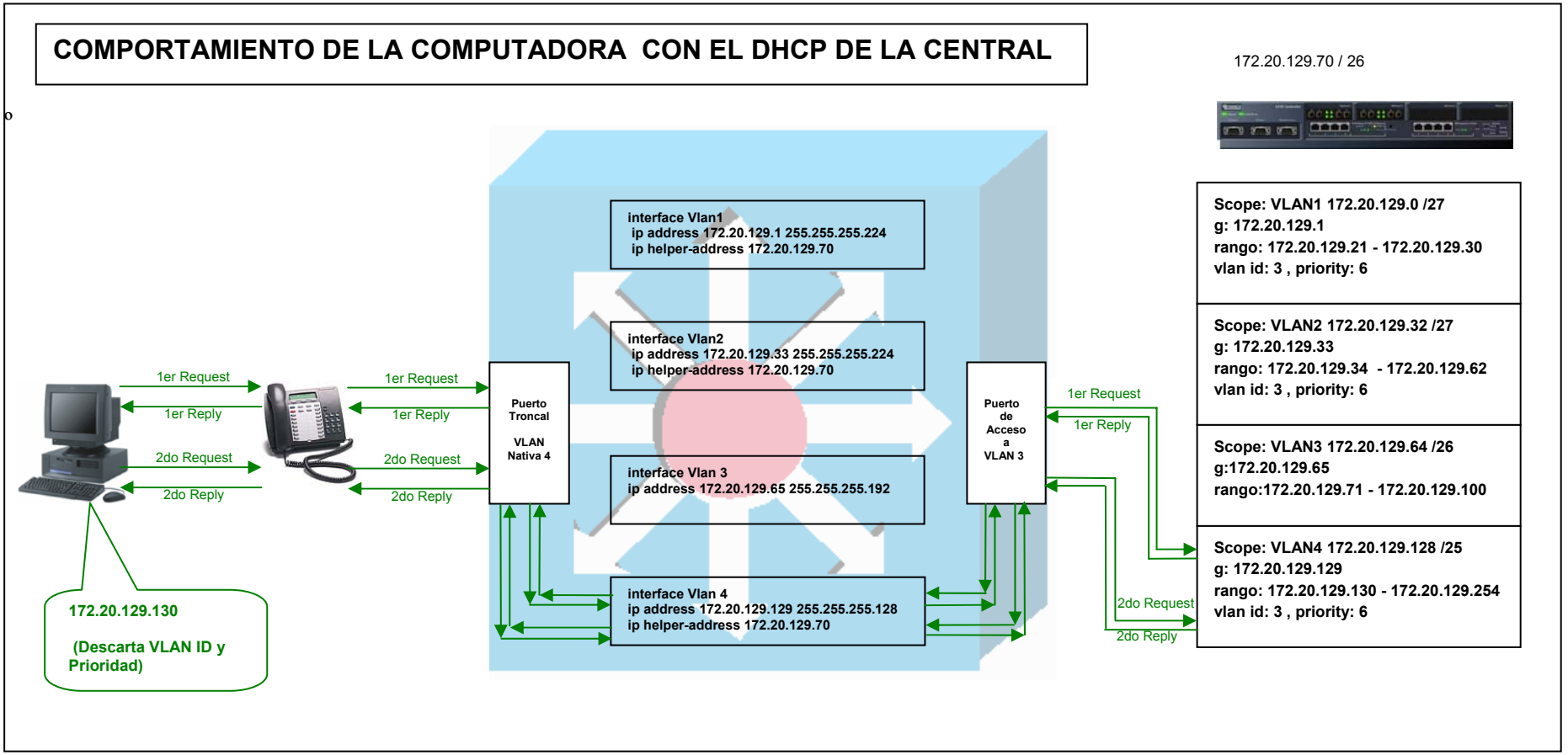


Figura 5.2 Comportamiento de la Computadora con el DHCP Mitel

5.1.2 Verificación del Teléfono en la VLAN de Voz

Configuro las interfaces de dos VLANs en el switch de capa 3, una VLAN para datos y otra VLAN de voz. Además habilito el enrutamiento en este switch, para que se puedan comunicar las VLANs.

El servidor DHCP se encuentra en la VLAN de voz (VLAN 3). A una computadora le conecto a un puerto de acceso a la VLAN de datos (VLAN 1) y a otra computadora le conecto a un puerto de acceso a la VLAN de voz (VLAN 3), ambas con su respectiva dirección IP, máscara y gateway, (configurado en forma estática). Además conecto un teléfono IP con computadora a un puerto troncal con VLAN nativa igual a la VLAN de datos (VLAN 1); los cuales van a recibir automáticamente la dirección IP, máscara y gateway del servidor DHCP. Además el teléfono IP recibe su VLAN ID y Prioridad.

Luego realizo ping desde ambas computadoras (en VLAN 1 y VLAN 3) a la dirección del teléfono IP (en VLAN 3) y efectivamente el ping es satisfactorio desde ambas computadoras, porque aunque el teléfono no se encuentre en la VLAN correcta, como existe enrutamiento entre las VLANs, no vamos a poder concluir nada; por lo tanto quitamos el enrutamiento y podemos observar que solo se mantiene un ping satisfactorio desde la computadora que se encuentra en la misma VLAN de voz, mientras que la otra computadora que se encontraba en la VLAN de datos dejó de tener un ping exitoso, lo cual nos lleva a concluir que **el teléfono IP se encuentra en la VLAN de voz. (LQQD).**

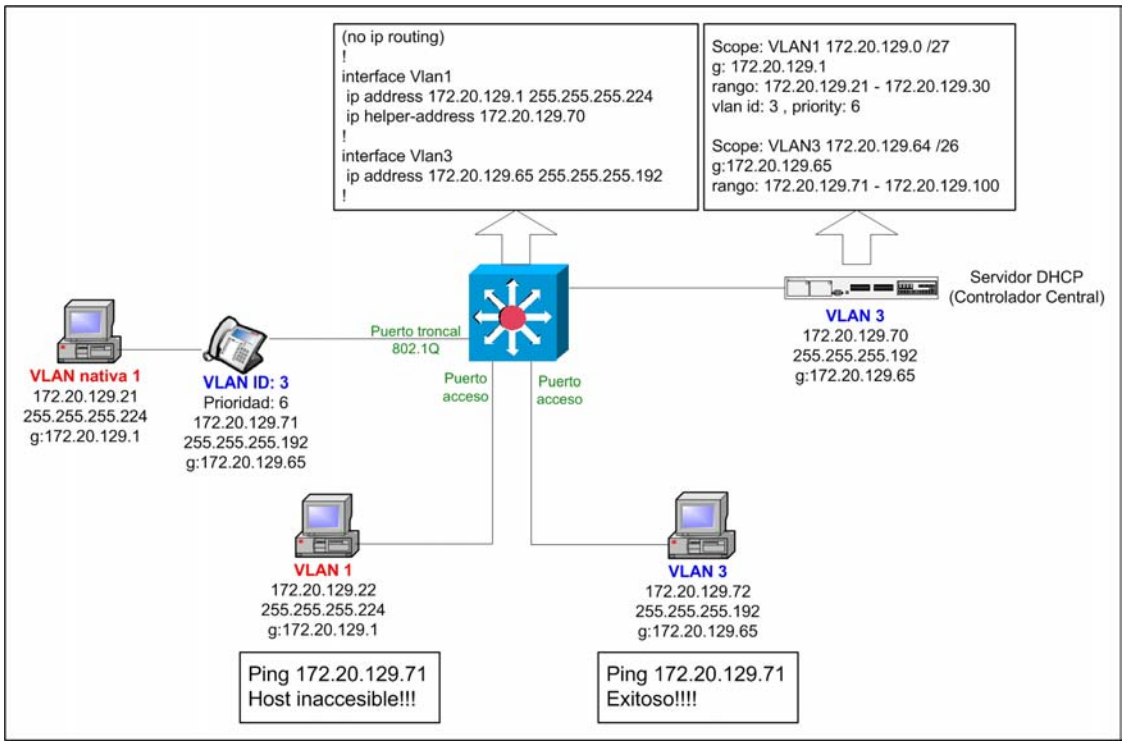


Figura 5.3 Verificación que el Teléfono está en la VLAN de voz

5.1.3 Verificación de la Computadora en la VLAN Nativa de Datos

Puedo verificar que la computadora se encuentra en la VLAN nativa de datos respectiva de diferentes formas, una forma es al igual que se hizo con el teléfono haciendo ping desde una computadora que se supone que está en la misma VLAN de datos y desde otra que no lo está, y cuando se quita el enrutamiento, solo la computadora que está en la misma VLAN de datos se mantiene con el ping exitoso. Y esto si sucede.

Otra forma de verificar es asignando una dirección IP que no corresponde a la VLAN nativa del puerto al cual están conectados el teléfono IP y la PC. Pero antes debemos hacer esta prueba con una PC conectada a un puerto de acceso a la VLAN de datos (VLAN 1) y asignarle una dirección IP que no corresponde a esta VLAN (en forma estática), para saber cual debe ser el comportamiento de la PC conectada al puerto troncal, y el resultado es que no puede hacer ping a ningún host; y efectivamente este es el mismo resultado con la computadora que se encuentra conectada al puerto troncal. Lo cual me permite concluir que **la computadora está en la VLAN nativa de datos respectiva**. **(LQQD).**

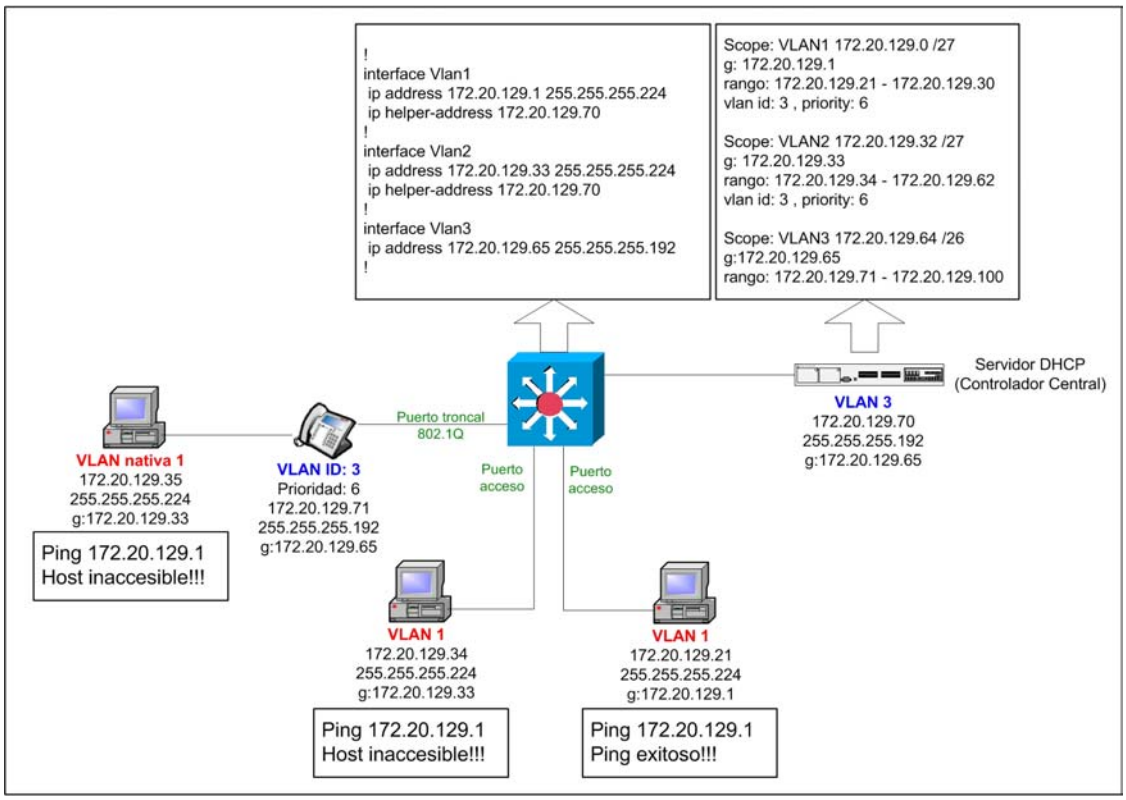


Figura 5.4 Verificación que la Computadora está en la VLAN Nativa de Datos

Pero la forma mas fácil de verificar que tanto el teléfono IP y la computadora están usando su respectiva VLAN cuando están conectados a un puerto troncal es usando los comandos de administración con privilegios: **show mac-address-table dynamic** que muestra las direcciones MAC, el puerto al cual están conectadas y las VLANs en las que están estos hosts; o directamente el comando **show mac-address-table interface** *interface-id,* en donde especifico el puerto del cual se desea conocer que hosts están conectados y en que VLAN se encuentran cada uno de ellos. Y para conocer de forma general que hosts o direcciones están en una VLAN determinada, utilizo el comando **show mac-address-table** *vlan –id.*

Otros comandos que también son de bastante ayuda para verificar la pertenencia de los hosts a su respectiva VLAN, además de la dirección IP asignada por el servidor DHCP, son los comandos de administración con privilegios **show arp,** que muestra las entradas a la tabla ARP, o el comando **show ip arp vlan** *vlan-id*, que muestra todos los hosts dentro de esa VLAN con su respectiva dirección IP y dirección MAC. Este último comando funciona para todas las VLANs en el switch que realiza la conmutación entre VLANs, es

decir en el switch multilayer ya sea el Catalyst 3550 o el 4500; mientras que en los otros switches solo es válido para la VLAN de administración.

5.1.4 Verificación de Rutas en el Router Vanguard Motorola

Para verificar las rutas aprendidas por el protocolo de enrutamiento RIP versión 2, en el router Vanguard Motorota, y saber específicamente si ha aprendido las direcciones de subred de cada una de las VLANs, declaradas en el switch multilayer para la red local; se sigue la siguiente secuencia: **Status/statistics -> Router stats -> IP stats**. Y aquí finalmente se elige la opción **IP Routing Table,** para ver las rutas aprendidas, es decir, la dirección de red destino, su máscara, la métrica, el tiempo de expiración y la interfaz o próximo salto a través del cual se conoce esta información. Ver Anexo 16, Tabla de Enrutamiento del Router Vanguard Motorola (220).

Para saber en forma específica, que direcciones IP de hosts ha aprendido el router se elige la opción **IP Routing Cache,** que muestra principalmente la dirección IP del host y la dirección y tipo de la interfaz que es el próximo salto a través del cual se conoce esta dirección IP.

5.1.5 Monitoreo del Desempeño del Switch Multilayer

Para verificar si las capacidades del Switch Cisco 3550 cumple con las exigencias de la red de Beaterio, se utilizó el programa Protocol Inspector de Fluke Networks y el programa de administración Cluster Managment Suit que es propio de estos switches Cisco. Esto se realizó especialmente porque este switch realiza el enrutamiento entre las VLANs, y además está conectado al router de acceso de la Frame Relay.

Es importante recalcar que las pruebas ejecutadas, no se han realizado sobre el diseño final de red planteado para Beaterio, pero al menos si se lo ha realizado sobre la columna vertebral de la actual red, que la constituyen los switches Cisco Catalyst: 3550 de Telecomunicaciones, 3500 XL de Jefatura y 2900 XL de Sucursal.

Básicamente se realizó el monitoreo del ancho de banda del switch 3550 de Telecomunicaciones, como se observa en la Figura 5.5.

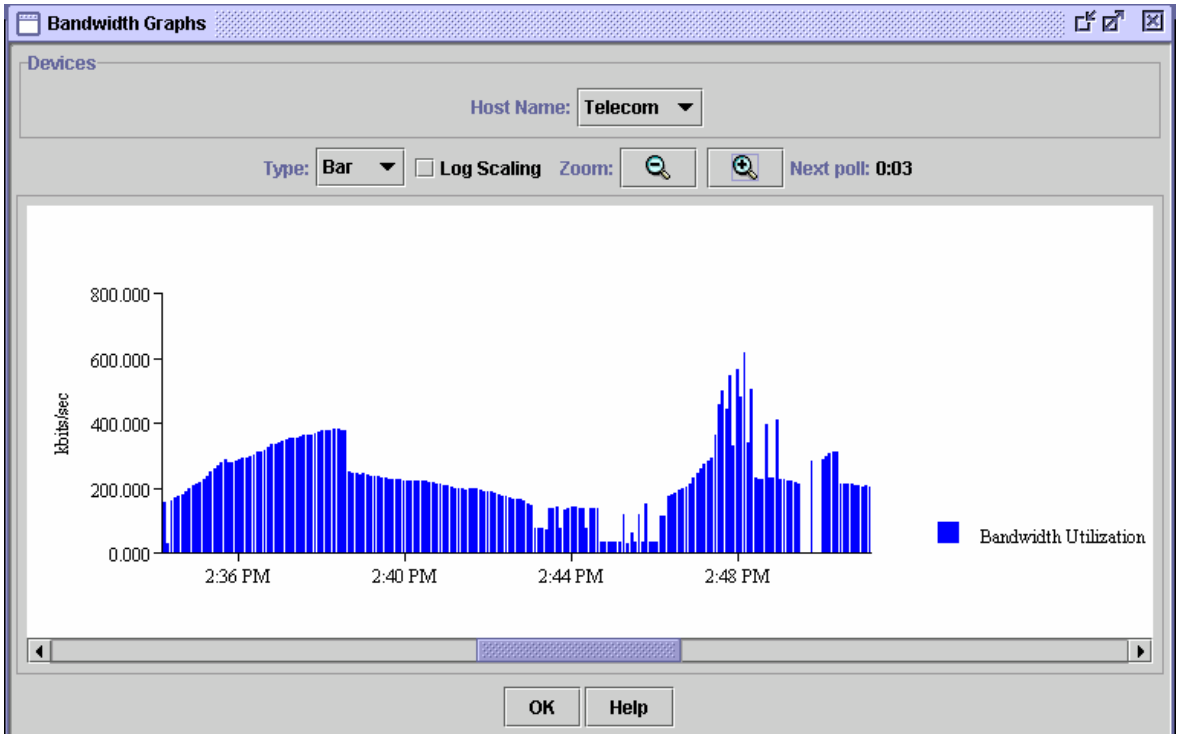


Figura 5.5 Monitoreo del Backplane del Switch Multilayer 3550 de la Red de Beaterio

Esta prueba se realizó en un día cotidiano de la semana, en un rango de tiempo que incluye las horas finales de labores, y se observó que el switch 3550 solamente utiliza un máximo de 0.5 Gbps de los 4.4 Gbps que tiene disponible en ancho de banda. Es decir el tráfico que circula en la red de Beaterio si es soportado con facilidad por el switch 3550.

Algo importante que también se puede concluir del monitoreo que se estaba realizando, fue que mientras se ejecutaba esta actividad por medio del programa Cluster Managment Suite, se genera una buena cantidad de tráfico por el intercambio de paquetes entre los dispositivos de interconexión de red y la estación de trabajo que realiza el monitoreo, lo cual obviamente consume los recursos de red. Esto ratifica que la propuesta de tener una sola VLAN para la administración de los switches y las máquinas que los administran, es correcta, para evitar que este tráfico interfiera con el resto de la red.

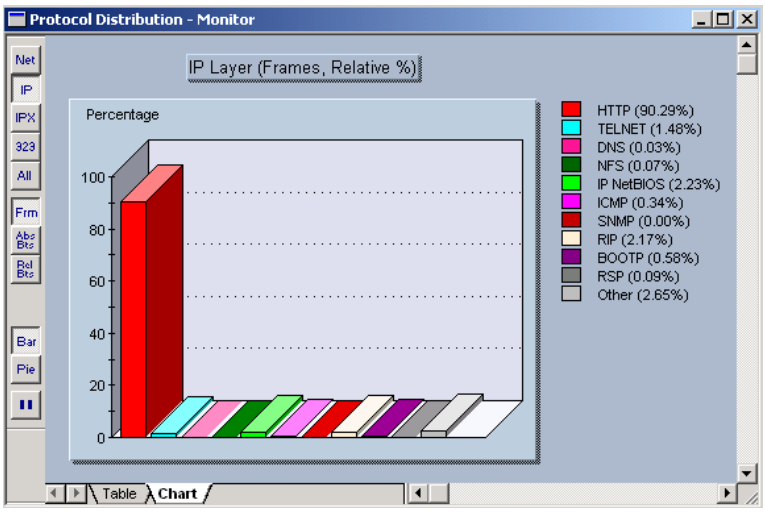


Figura 5.6 Monitoreo del tipo de tráfico

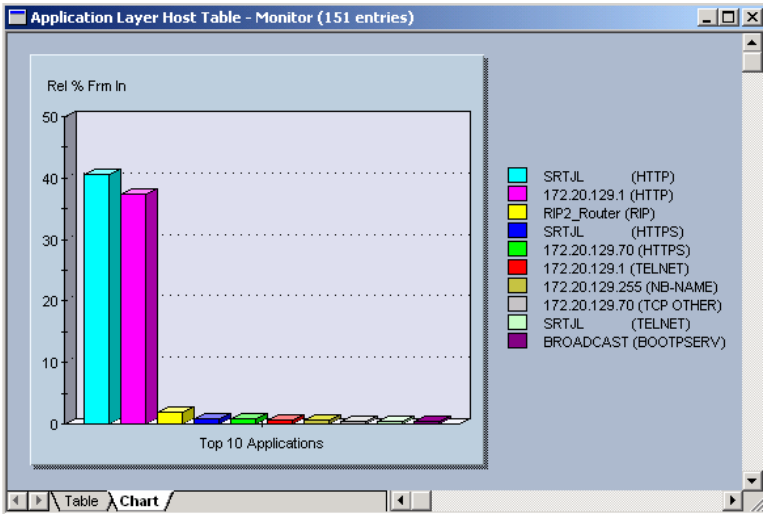


Figura 5.7 Monitoreo de Hosts

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- El empleo de VLANs, mejora el desempeño de la red de la Matriz, debido a que se han incrementado el número de dominios de broadcast y el tamaño de estos dominios es menor. Otra importante razón por la cual se mejora el desempeño de esta red es porque se ha realizado una adecuada segmentación de las VLANs en base al flujo de tráfico, es decir se han agrupado los servidores de grupo de trabajo con los usuarios que generalmente los utilizan; caso contrario no tiene mucho sentido implementar VLANs, es decir si solamente existen servidores empresariales en la red local, no es muy conviene implementar VLANs porque realmente no van a mejorar el desempeño de la red, e incluso los usuarios siempre deberán utilizar enrutamiento para llegar a la VLAN donde se encuentran esos servidores, y además se añade mayor latencia a los paquetes porque estos deberán ser analizados hasta capa 3.

- La red de Beaterio, obviamente también goza del beneficio del mejoramiento del desempeño de la red, por haber divido en varios dominios de broadcast a esta red, pero esto no es muy notorio debido a que esta red es pequeña, y la razón más importante es porque los usuarios de esta red para comunicarse con los servidores o acceder a cualquier servicio, igual tienen que cruzar la red de área extendida Frame Relay.

- Por medio de la configuración de VLANs estáticas se provee de flexibilidad y escalabilidad a la red de la Matriz y Beaterio, porque permiten fácilmente la adición, movimiento o cambio de las estaciones de trabajo, y a la vez mantener los otros beneficios que tienen las VLANs.

- La implementación de VLANs estáticas ofrece implícitamente un control del movimiento de los usuarios, porque para realizar cualquier movimiento de estaciones de trabajo, se debe conocer a quién pertenece la estación de trabajo, para según esto configurar adecuadamente el puerto del switch al cual va ir conectado el host, y así asignarle correctamente la respectiva VLAN (nativa).

- La configuración de VLANs propuesta tanto para la red de la Matriz como para la red de Beaterio por defecto no ofrecen seguridad, porque está habilitado el enrutamiento entre todas las VLANs (excepto la VLAN de Filiales y la VLAN de la Extranet), y además el requerimiento por parte de la Unidad de Sistemas y Telecomunicaciones para configurar las VLANs es tener comunicación entre todas ellas, hasta que se realice un análisis más profundo y detallado de las seguridades que deben implementarse, lo cual no es un objetivo de este proyecto. Pero es de importancia para este proyecto ofrecer el mejor diseño de VLANs para estas redes, por lo tanto los diseños que se proponen si ofrecen la factibilidad de la implementación de seguridades futuras.

- Es mejor utilizar puertos enrutados (capa 3) en lugar de puertos conmutados (capa 2), para conectar los routers de acceso al switch multilayer, porque no extendemos el dominio de broadcast de cualquier VLAN de forma innecesaria y además se pueden configurar seguridades en estos switches para estos accesos remotos que no siempre son confiables, a pesar de que sean parte de la propia red de Petrocomercial.

- Se mejora el servicio telefónico IP dentro de las redes locales de la Matriz y de Beaterio debido a que todos los teléfonos IP y la Central Mitel que los administra, se encuentran dentro de una sola VLAN, y por lo tanto estos no se ven afectados por el tráfico de datos que se encuentra en otras VLANs.

- El tráfico de voz también mejora porque la prioridad configurada para éste tráfico con el estándar IEEE 802.1p, es mayor a la del tráfico de datos, lo cual le indica a los switches poner en las colas que tienen mayor preferencia para la transmisión de estas tramas.

- Se determinó hacer el diseño de VLANs y el rediseño de red solo en la Matriz y el Beaterio porque son las dos únicas redes locales que lo justifican y admiten; debido a que las otras redes tienen una cantidad hosts muy pequeña y la mayor parte de sus equipos no soportan la configuración de VLANs; además no se propone la compra de nuevos equipos porque estas redes tan pequeñas no lo justifican.

- Los principales beneficiados de este proyecto son los usuarios, porque obtendrán una confiable y rápida comunicación con los servidores al igual que en la transferencia de archivos o cualquier aplicación análoga.

- Para definir el diseño adecuado de VLANs, se debe encontrar un balance entre lo que es el desempeño de la red y la seguridad o filtros de tráfico que se apliquen sobre ésta.

- El protocolo VTP (*Virtual Trunking Protocol*) es de gran ayuda para no tener que configurar las VLANs en todos los switches, simplemente se debe configurar las VLANs en el switch que esté en modo servidor, y el resto de switches debe estar en modo cliente.

- Los diseños propuestos tiene un buen nivel de confiabilidad porque tiene enlaces redundantes, pero por lo mismo es necesario habilitar el protocolo *Spanning-Tree* para evitar los lazos de tráfico y por ende que caiga la red.

- Este proyecto sirve como base para el diseño y configuración de VLANs de cualquier red local, obviamente tomando en cuenta las necesidades y características de la empresa.

6.2 RECOMENDACIONES

- Establecer como **política de administración**, que solo las personas que administran y dan mantenimiento a la red tengan acceso a los equipos de interconexión de red, especialmente para la tarea más cotidiana que es el ingreso, salida o cambio de hosts, para que éste personal con el conocimiento claro de la distribución de VLANs, configure adecuadamente los puertos de los switches.

- Comprar tarjetas Gigabit Ethernet para los Servidores e iSeries, para conectarlos con cable UTP cat-6 bajo el estándar 1000 Base-T al Switch de Core y así mejorar considerablemente el rendimiento de la red y a su vez aprovechar los puertos 10/100/1000 Base-T del switch Cisco 4500. Otra alternativa es comprar tarjetas Gigabit Ethernet para fibra óptica bajo el estándar 1000 Base-SX, lo que implica la compra de un módulo adicional de puertos GBIC para el switch Cisco 4500.

- Comprar un software de administración para el Switch Cisco Catalyst 4500 Series.

- No implementar muchas listas de acceso en los switches multilayer 4500 y 3550 que se conectan a los routers de acceso, porque aunque los diseño ofrecen esta facilidad, es preferible que los filtros de tráfico se realicen en los propios routers de acceso. Y así conseguir que estos switches funcionen más en la capa de core de la LAN que en la capa de distribución, porque incrementan la latencia de los paquetes en lugar de hacer una conmutación rápida de los mismos.

- Para el nuevo diseño de la red de la Matriz, se recomienda tender fibra óptica de 6 hilos multimodo entre el quinto y segundo piso, para tener hilos de fibra de respaldo.

- Habilitar el protocolo Spanning-Tree en todos los switches de la red, porque los diseños de red propuestos tienen enlaces redundantes.

- Si se desea utilizar puertos de acceso para conectar los teléfonos IP, entonces no configurar las opciones del VLAN ID ni Prioridad del DHCP de la Central IP Mitel.

- Realizar un tendido de cableado estructurado debidamente certificado para mejorar la confiabilidad de los diseños de red propuestos.

- Instalar un servidor DHCP exclusivo para las computadoras en la red de Beaterio, porque si bien esta red es pequeña, no es conveniente estar utilizando el mismo DHCP de la central Mitel tanto para los teléfonos como para las computadoras.

- En un dominio VTP, siempre es conveniente instalar a un nuevo switch como cliente VTP, y asegurarse que el número de registro de configuración es inferior al que tiene el servidor del dominio, porque caso contrario es posible que el nuevo switch envíe una nueva base de datos VTP a todos los otros switches incluyendo al servidor, borrando así todas las VLANs existentes en el dominio.

REFERENCIAS BIBLIOGRÁFICAS

- Mitel Networks Coorporation, **Integrated Communications Platform 3300 - Technician's Handbook**, Release 3.3, Abril del 2003, 287 págs.

- Mitel Networks Coorporation, **Integrated Communications Platform 3300 - Guía de Información General**, 2002, 117 págs.

- Mitel Netwotks Coorporation, **LAN Design Guidelines for the Implementation of MN3300 Platforms,** Mayo del 2002, Canada, 24 págs.

- Cisco Systems, **CCNA 1: Networking Basics v3.1**

- Cisco Systems, **CCNA 2: Routers and Router Basics v3.1**

- Cisco Systems, **CCNA 3: Switching Basics and Intermediate Routing v3.1**

- Cisco Systems, **CCNA 4: WAN Technologies v3.1**

- LAMMLE, Todd, **Cisco Certified Network Associate Study Guide**, 4ta edición, 2004 Sybex Inc, 606 págs.

- Cisco Systems, **Catalyst 3550 Multilayer Switch Software Configuration Guide**, Cisco IOS Release 12.1(14)EA1.

- Cisco Systems, **Catalyst 2900 Series XL and Catalyst 3500 Series XL Software Configuration Guide**, Cisco IOS Release 12.0.

- Cisco Systems, **Catalyst 4500 Series Software Configuration Guide**, Cisco IOS Release12.1(20)EW.

- Cisco Systems, **How to configure intervlan routing on layer 3 switches**, 9 Enero del 2005, 8 págs.

- Anritsu Company, **How Did LANs Evolve to Multilayer Switching?**, 1998, 10 págs.

- PACHÓN, Alvaro, **La evolución en la arquitectura de las redes**, Departamento de Redes y Comunicaciones Universidad Icesi-I2T, 12 págs.

- http://www.vanguardms.com/documentation, **IP Routing Basics.**

- http://www.vanguardms.com/documentation, **IP Configuration.**

- http://www.vanguardms.com/documentation, **Statistics.**

ANEXOS

ANEXO 1: Servidores y Firewall

SERVIDORES Y FIREWALL

PCORED	PCORED1	PCORED2	PCORED4
Serv. Compac Proliant ML 350 S.O: Windows 2000 Server APL: Lotus Domino (Correo Interno, Control Documental 2004, Odenes de Pago, Viáticos, Help Desk, Inventario, Juicios), IIS, TSM, Norton, DHCP Server, DNS, Primary Controller.	Serv. IBM Netfinity 3500 864430U S.O: Windows 2000 Server APL: DNH, SRI, Sistemas de oferentes, Auditoría, IIS, Symentec Web Security, Norton Antivirus, Domino ID´s, Java Development Kit	Serv. Compac Proliant ML350 S.O: Windows 2000 Server APL: Pruebas de W 2003 Server YA NO FUNCIONA!!!	Serv. IBM Netfinty 7000 M10 S.O: Windows 2000 Server APL: DataWareHouse, Bussiness Object, DB2 UDB 7.2, Norton Antivirus TSM Manager for DB2, TSM Manager Client.
PCORED5	**PCORED6**	**PCORED7**	**PCOWEB**
Serv. IBM Netvista S.O: Windows 2000 Server APL: DB2 UDB 7.2 (Backup Pcored4)	Serv. Compac Proliant DL580 S.O: Red Hat Linux 7.3 APL: WEBSPHERE, TSM Server YA NO FUNCIONA!!!	Serv. Compac Proliant ML350 S.O: Red Hat Linux 9.0 APL: Servidor de pruebas de Linux, Domino 6.5, Control Documental 2005	Serv. Compac Proliant ML350 S.O: Windows 2000 Server APL: IIS(Página Web), Lotus Domino(Servidor de Correo Externo), Symantec Sistem Center, Norton Antivirus, Sitios FTP

PCO1	PCO2	PCO8	PCO9
S.O: OS/400 V5R2 Recursos Humanos, Activos Fijos, Contratos, Maintraker	S.O: OS/400 V5R2 Contabilidad y presupuesto (CGIFS) APL: Ambiente de Desarrollo de: Comercialización Interna y Movimiento de Productos	S.O: OS/400 V5R2 APL: Comercialización Interna,Movimiento de Productos	S.O: OS/400 V5R2 APL: Base de Datos del Sistema Comercialización Interna (Rediseño)

FIREWALL
Serv. IBM RS6000
S.O: AIX 4.5.9
APL: SecureWay Firewall 4.2
POLITICAS
BASE DE DATOS:
SRI
MEM
SOTE
PCORED4
CORREO:
Servidor Interno
Petroecuador
INTERNET:
Todas las Sucursales
y Terminales
TELNET:
PCO8 (Ministerio de Energía y Minas)
FTP:
PCORED4
PCOWEB

Sistemas Oferentes y Auditoria: de Petroecuador
DNH: Dirección Nacional de Hidrocarburos
Maintraker: Inventarios de Materiales

S.O. Sistema Operativo
APL:aplicación

ANEXO 2: Puertos Asignados a Equipos y Servidores

PUERTOS ASIGNADOS A EQUIPOS Y S E R V I D O R E S

Swicth Modelo	CISCO CATALYST 3500 XL
S/N	
Piso	5to
Etiqueta	SW 155C

Puerto	1:01	2:01	3:01	4:01	5:01	6:01	7:01	8:01
Equipo		ROUTER IBM 2216-400 (Corazón, Chalpi)	ROUTER IBM 2210 Acceso Remoto Dial Up	SWITCH / ROUTER IBM 8274 (DE BAJA)	Router Morola 6455 Nodo 200		Servidor Compaq de correo interno Lotus, DHCP, DNS	UPLINK A SW152C
MAC Adress			0004.acca.7458				00-50-8B-E7-FE-20	
IP Adress		172.20.64.2	172.20.64.4	172.20.64.10	172.20.64.11		172.20.64.20	
Extensión							PCORED	
Pto. Red		ROUTER 2216	ESM SWITCH		#2 COMM'S		#6	3
Dependencia		Sistemas	Sistemas	Sistemas	Telecomunicaciones		Sistemas	
Responsable								

Puerto	9:01	10:01	11:01	12:01	13:01	14:01	15:01	16:01
Equipo	ROUTER CISCO 800 series (Riobamba, Cuenca, Guayaquil)	Servidor Compaq (PROLIANT -DL580) Websphere	Firewal Linux de prueba (no existe)	Servidor IBM de Red Usuarios, Web interna, SRI, DNH	Servidor IBM Netfinity 7000 M10, DWH	Servidor IBM Netfinity 7000 M10, DWH		FIREWALL IBM AIX
MAC Adress	00b0.c28d.fd8a	0002.a55c.f574	00-10-5A-A4-99-E9	00-60-94-B9-BB-6E		0010.b548.d830		0004.ac17.0e32
IP Adress	172.20.64.3	172.20.71.9	200.24.212.19	172.20.71.21		172.20.64.24		172.20.64.6
Extensión		PCORED6	PCOFIREWALL	PCORED1	RESPALDO	PCORED4		LAN INTERNA
Pto. Red		#3		#2	1N	2N		Rojo
Dependencia	Sistemas	Sistemas	Sistemas	Sistemas	Sistemas	Sistemas		Sistemas
Responsable								

Puerto	17:03	18:03	19:03	20:03	21:02	22:02	23:02	24:02
Equipo		FIREWALL IBM AIX		Comunicaciones con Filiales Switch 3COM (pos)	FIREWALL IBM AIX	ROUTER IBM 2210 para Internet, SRI y DNH	Servidor Compaq de correo externo, Web, Internet	
MAC Adress		0002.55af.1d7e			0004.ac3e.e44e	0004.acca.17c8	0050.8be9.05e0	
IP Adress		10.10.10.17			200.24.212.22	200.24.212.17	200.24.212.21	
Extensión		LAN FILIALES			LAN EXTERNA		PCOWEB	
Pto. Red		#5		#1 COMM'S	Azul		#1	
Dependencia		Sistemas		Telecomunicaciones	Sistemas	Sistemas	Sistemas	
Responsable								

SW159C puerto 12	SW159C puerto 20	SW157T puerto 4	SW159C puerto 17	SW154C puerto 18
Servidor Compaq (Windows 2003 Server en prueba)	Servidor IBM (Windows 2003 Server en prueba)	Servidor IBM Backup del PCORED4	Impresora IBM Infoprint 1145	Servidor Compaq, Linux en prueba
00-50-8B-E9-0A-7E	00-09-6B-BA-33-20	000d.606b.61ee	0004.00e2.ffae	00-01-03-CD-80-85
ip: 172.20.64.52	ip: 172.20.64.53	ip: 172.20.64.55		ip: 172.20.64.57
PCORED2	PCORED3	PCORED5		PCORED7
0221	0223		0222	0224
Sistemas	Sistemas	Sistemas	Sistemas	Sistemas

ANEXO 3: Computadoras de la Red la Matriz

COMPUTADORAS DE LA RED LA MATRIZ								
Piso	Nombre de la Computadora	MAC Address	Usuario	Departamento	Unidad	Switch	Puerto	Observación
1er	KANCT	00096b6f79d8	TORRES CAMILO	Administración de Negocios Propios	Comercializadora	SW112T	5	
1er	KANJT	00096bba3313	TOBAR JISELA	Administración de Negocios Propios	Comercializadora	SW129C	23	
1er	FCCAN	000d9d4a0bd6	NEGRON ARMANDA	Crédito y Cobranzas	Finanzas	SW129C	5	
1er	FCCCC	00105aa499ea	CREDITO Y COBRANZAS	Crédito y Cobranzas	Finanzas	SW122C	10	
1er	FCCCD	00096bba3bff	DIAS CONSUELO	Crédito y Cobranzas	Finanzas	SW112T	1	
1er	FCCED	0002a536e7f9	DAVILA ERIKA	Crédito y Cobranzas	Finanzas	SW122C	14	
1er	FCCJR	0002555dc36c	RUANO G.JAHEL M.T.	Crédito y Cobranzas	Finanzas	SW112T	2	
1er	FCCMC	00105aa62003	CASTANEDA E.MIRIAM A.	Crédito y Cobranzas	Finanzas	SW121C	15	
1er	FCCMR	0009.6bba.33e6	LIBRE	Crédito y Cobranzas	Finanzas	SW121C	5	
1er	FCCRP	00096bba32b7	PAREDES M.ROSA L.	Crédito y Cobranzas	Finanzas	SW129C	16	
1er	FCCMM	00096b041dd3	MORENO R. MARITZA A.	Crédito y Cobranzas	Finanzas	SW129C	24	
1er	FSGFG	0002.a556.de40	GUZMAN P.JAIME F.	Seguros y Garantías	Finanzas	SW112T	7	172.20.64.44
1er	FSGMT	0004.ac53.787d	TAPIA M.MARGARITA E.	Seguros y garantías	Finanzas	SW121C	11	172.20.64.41
1er	FSGMV	000d.9d4a.0899	VILLALBA MARIA L.	Seguros y Garantías	Finanzas	SW112T	6	172.20.64.42
1er	FSGPB	0002a556ab3c	BURBANO PATRICIA	Seguros y garantías	Finanzas	SW121C	13	
1er	FSGXO	0004.ac53.4f94	OBANDO S.XIMENA L	Seguros y Garantías	Finanzas	SW112T	4	
1er	FSGYC	00096bba331f	CORONEL G.YOLANDA R.	Seguros y garantías	Finanzas	SW112T	3	
1er	MCLGP	0004ac535607	PEÑA GERARDO	Compras Locales	Materiales	SW111I	14	
1er	MCLGT	0002a536ebff	TORRES P.GUSTAVO J.	Compras Locales	Materiales	SW122C	19	
1er	MCIOP	0002553b8502	PACHARD A.GIL O.	Compras Locales	Materiales	SW129C	15	
1er	MCLRV	0002a536a6d1	VALAREZO L.RODRIGO A.	Compras Locales	Materiales	SW129C	6	
1er	MCLZR	0002555dad64	RUEDA V.ZAYDA M.	Compras Locales	Materiales	SW111I	10	
1er	MCMBA	0002a53553e0	ARANA F.BIBIANA R.	Control de Materiales y Bodega	Materiales	SW129C	21	
A	MCMBA1	000475aa83c4	ARANA F.BIBIANA R.	Control de Materiales y Bodega	Materiales	SW111I	23	
1er	MCMCV	00096b6f7991	VILLAVICENCIO S.CHRIS D.	Control de Materiales y Bodega	Materiales	SW102I	12	
1er	MCMMA	00096bba3bf3	ARCOS J.MONICA E.	Control de Materiales y Bodega	Materiales	SW111I	9	
1er	MCMMG	0002a536eca9	GALLARDO T.MIRIAM S.	Control de Materiales y Bodega	Materiales	SW122C	17	
1er	MIMDL	00096bba402a	LOAYZA L.DIANA M.	Importaciones	Materiales	SW111I	7	
1er	MIMIMP	0002553b8750	PONTON G.IVAN M.	Importaciones	Materiales	SW129C	17	
1er	MIMIP	00096bba3f12	LIBRE	Importaciones	Materiales	SW111I	12	
1er	MIMNP	0002553b876d	PINTO R.NOE J.	Importaciones	Materiales	SW111I	8	
1er	MIMSP	00096bba327b	PAZMIÑO P.SILVIA M.	Importaciones	Materiales	SW121C	21	
1er	AMAGL	0050bacd04f4	GONZALO LEÓN	Materiales	Materiales			Desconectada
1er	AMAMU	0004ac5377f9	UTRERAS MIRIAM	Materiales	Materiales	SW121C	19	
2do	CABAA	00096bba3408	AGUAS M.AMPARO DEL C.	Abastecedora	Abastecedora	SW122C	6	
2do	CABGA	0004ac536d46	ACOSTA H.GENOVEVA DE L.	Abastecedora	Abastecedora	SW129C	19	
2do	BCOGV	0002a536ec7b	VELASQUEZ C.GALO E.	Coordinación Operativa	Abastecedora	SW122C	13	
2do	BCOJG	00096b6f7a06	GARCIA O. JOSE R.	Coordinación Operativa	Abastecedora	SW121C	6	
2do	BCOLG	0002a536ec26	GUERRERO G. LENIN G.	Coordinación Operativa	Abastecedora	SW122C	5	
2do	BCOMM	0004ac5377c9	MORALES MAXIMO	Coordinación Operativa	Abastecedora	SW129C	14	
2do	BCOPS	0002a536a76c	SOLANO C. PETRONIO I.	Coordinación Operativa	Abastecedora	SW122C	20	
2do	BFVCM	00003961469a	MISSURA CHRISTIAN	Facturación y Ventas	Abastecedora	SW129C	8	Portatil Particular
2do	BFVCA	0002553b89b3	ARIAS A.CARLOS P.	Facturación y Ventas	Abastecedora	SW122C	18	
2do	BFVLJ	0002a536ecab	JAYA U.LUIS A.	Facturación y Ventas	Abastecedora	SW129C	11	
2do	BFVPE	00096b6f74b5	EGAS PAUL	Facturación y Ventas	Abastecedora	SW121C	4	
2do	BFVVZ	0002a536ec84	ZAMBONINO M.VICTOR H.	Facturación y Ventas	Abastecedora	SW121C	9	
2do	BFVXT	0004ac5375d3	TOLEDO M.XIMENA DEL R.	Facturación y Ventas	Abastecedora	SW122C	1	
2do	BLCCF	0002a536a760	FLOR CECILIA	Liquidación y Consolidación de Cuentas	Abastecedora	SW129C	9	
2do	BLCFH	0002a536ecc3	HINOJOSA R.FERNANDO	Liquidación y Consolidación de Cuentas	Abastecedora	SW129C	3	
2do	BLCKV	00096bba41ca	VELASCO KRUPSKAYA	Liquidación y Consolidación de Cuentas	Abastecedora	SW129C	10	
2do	BLCRR	00096b6f7cd3	RAMIREZ G.RAUL R.	Liquidación y Consolidación de Cuentas	Abastecedora	SW122C	3	
2do	AFIFT	0002553b8df2	TORRES A.FLOR M.	Finanzas	Finanzas	SW129C	7	
2do	AFIJP	000d606b5a20	PUNGACHO JORGE	Finanzas	Finanzas	SW122C	12	
2do	AFICA	000d606b6281	ARTIEDA CARLOS	Presupuesto	Finanzas	SW122C	16	
2do	FPRIG	0002553b83b2	GARCIA INES	Presupuesto	Finanzas	SW121C	7	
2do	FPRML	00096bba3efa	LOZADA F.MARIA F.	Presupuesto	Finanzas	SW121C	3	
2do	FPRRP	00096bba3773	PESANTES ROCIO	Presupuesto	Finanzas	SW122C	11	
3er	CKOEP	00096bba4152	PADILLA V.AMPARO	Comercializadora	Comercializadora	SW131T	2	
3er	CKOGA	0002a536a71b	AGAMA GERMAN	Comercializadora	Comercializadora	SW153C	11	

Piso	Nombre de la Computadora	MAC Address	Usuario	Departamento	Unidad	Switch	Puerto	Observación
3er	CKOPP	00096b6f74d2	PALOMINO L.PATRICIA A.	Comercializadora	Comercializadora	SW122C	7	
3er	CKOSM	0002555da93c	MESIAS SORAYA	Comercializadora	Comercializadora	SW153C	16	
3er	CKOYV	00096bba3321	VERA G.ROSALBA Y.	Comercializadora	Comercializadora	SW131T	4	
3er	GCCMM	00080d179007		Comercializadora	Comercializadora	SW131T	#	CKOMM, Portatil particular
3er	KCOOE	00096bba237b	ERAZO A.OSWALDO A.	Coordinación Operativa y Ventas	Comercializadora	SW131T	5	
3er	KCOSY	0002a536a6ca	YONFA C.SANDRA J.	Coordinación Operativa y Ventas	Comercializadora	SW131T	3	
3er	KMAFS	0002553b866d	SAUD FERNANDO	Mercadeo y Atención al Cliente	Comercializadora	SW151C	3	
3er	KMAIB	0002555db077	BAEZ IVAN	Mercadeo y Atención al Cliente	Comercializadora	SW152C	13	
3er	KMAVJ	00096bba3304	JURADO S.VILMA DEL R.	Mercadeo y Atención al Cliente	Comercializadora	SW151C	5	
3er	VGNAC	00055d26c127		Gerencia Regional Norte	Gerencia Regional Norte	SW122C	9	
3er	VGNCR	0010605b80b8	RAMIREZ CARLOS	Gerencia Regional Norte	Gerencia Regional Norte	SW153C	10	
3er	VGNEG	0002a565e400	GARCIA S.GIOVANNA E.	Gerencia Regional Norte	Gerencia Regional Norte	SW153C	20	
3er	VGNGF	00096bba331e	FIALLO C.JAIME G.	Gerencia Regional Norte	Gerencia Regional Norte	SW153C	19	
3er	VGNJF1	000039863ee9		Gerencia Regional Norte	Gerencia Regional Norte	SW154C	14	
3er	GSCHC	00096bba3831	CEVALLOS M.HILDA P.	Subgerencia de Comercialización	Subgerencia de Comercialización	SW153C	22	
3er	GSCMD	0002553b8792	DURANGO L. MARTHA C.	Subgerencia de Comercialización	Subgerencia de Comercialización	SW152C	4	
4to	SSAAA	0004ac536e01	AMANCHA AMPARO	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW141I	3	
4to	SSAAG	0002a5355209	GRANIZO AMPARO	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW149C	1	
4to	SSABR	000d.606a.f7cd	RIVERA S.BLANCA M.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	16	
4to	SSACS	0002553b8bdd	SALAZAR R.CRISTOBAL E.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	9	
4to	SSADI	000d606b59e3	IZA DIEGO	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW149C	11	
4to	SSAFC	00096b6f7b49		Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	8	
4to	SSAFL	00096b6f7da6	LUCERO FERNANDA	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW141I	5	
4to	SSAGP	000d606b58ca	PEREZ H.GINA M.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW149C	12	
4to	SSAJD	000d606b62d5	DELGADO G.JOSE J.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	19	
4to	SSAJM	00096bba377e	MURILLO C.JIMMY HECTOR V.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW152C	21	
4to	SSAJV	0002555dc0a5	VILLACIS M.JENNY L.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	3	
4to	SSALG	00096bba34c7	GRIJALVA R.LUIS F.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	1	
4to	SSALOV	00096bba3316	VILLAVICENCIO G.LUIS O.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW151C	8	
4to	SSALV	0002a5568d30	VILLAVICENCIO G.LUIS O.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW141I	16	
4to	SSAPC	00096bba3671	CARRERA PAOLA	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW141I	6	
4to	SSARB	0002555db639	BECERRA RAFAEL	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW149C	10	
4to	SSARC	000d606af7b0	CHICAIZA A.ROSA M.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	12	
4to	SSARG	000d606b5a16	GALLO L.ROBERTH F.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW152C	14	
4to	SSAFT	000d.606b.6316	TAPIA C.FERNANDO G.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	11	172.20.64.31
4to	VLECG	0002551d267a	GARCIA CHRISTIAN	Legal Vicepresidencia	Vicepresidencia	SW159C	14	
4to	VLECT	00096bba3bc0	TORRES M.CONSUELO E.	Legal Vicepresidencia	Vicepresidencia	SW153C	15	
4to	VLEVG	00096b61defc	GARCIA V.VINICIO W.	Legal Vicepresidencia	Vicepresidencia	SW153C	13	
4to	VPFAG	00096bba3768	GUANO M.ANA C.	Planificación y Finanzas	Vicepresidencia	SW149C	4	
4to	VPFBC	00096bba32f0	CARRION A.BYRON E.	Planificación y Finanzas	Vicepresidencia	SW149C	5	
4to	VPFDP	00096bba3305	PAZMIÑO G.DORA M.	Planificación y Finanzas	Vicepresidencia	SW149C	7	
4to	VPFEL	00096bba3ef0	LOMBEIDA M. EDGAR R.	Planificación y Finanzas	Vicepresidencia	SW159C	19	
4to	VPFFG	00096bba400a	GUARDERAS FERNANDO	Planificación y Finanzas	Vicepresidencia	SW149C	6	
4to	VPRMC	0002a536ec79	DE LA CRUZ G.MARTHA Z.	Programación	Vicepresidencia	SW151C	10	
4to	VPRMI	00096bba3bc9	IZQUIERDO MIGUEL	Programación	Vicepresidencia	SW151C	6	
4to	VPRMR	00096bba3f08	RIVADENEIRA M.MARTHA V.	Programación	Vicepresidencia	SW159C	5	
4to	VPRNA	00096bba3395	ALARCON C.NICOLAS A.	Programación	Vicepresidencia	SW159C	21	
4to	VPRNG	00096bba3471	GUERRA N.NANCY E.	Programación	Vicepresidencia	SW159C	22	
4to	VPRPR	0002a536ec73	REYES PATRICIA	Programación	Vicepresidencia	SW149C	3	
5to	GSIRMR	0006.1bc4.395f		Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW157T	1	
5to	SIPLQ	0002555db078	QUILCA LUIS	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW151C	4	
5to	SIPMC	00096bba3390	CANGAHUAMIN J.MAYRA P.	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW152C	10	
5to	SIPOB	0002553b89b8	BUSTOS B.OSCAR M.	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW152C	18	
5to	SIPPS1	00d0592e4ea3	SALAZAR PATRICIO	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW152C	20	
5to	SIPRR	00096bba3382	ROMERO V.ROSA M.	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW152C	5	
5to	SRTAV	0002555db62b	VILLALVA ARACELLY	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW157T	2	
5to	SRTCP	00096bba3383	PAEZ GUSTAVO	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW151C	19	
5to	GSIGM	00096bba3bc3	MANCHENO O.GUILLERMO O.	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW153C	8	
5to	GSIJS	00096b90b709	SALINAS H. JAQUELINE M.	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW152C	2	
5to	GSISL	00096bba33ab	LARA F.SANDRA M.	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW152C	9	
5to	SRTHR	0002.555d.b32d	PAEZ CESAR G.	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW157T	3	
5to	SSTEH	00096bba3cd7	HOLGUIN ELENA	Soporte Técnico y Mantenimiento	Sistemas y Telecomunicaciones	SW154C	6	
5to	SSTIC	0002555dba09	CORNEJO R.IVAN F.	Soporte Técnico y Mantenimiento	Sistemas y Telecomunicaciones	SW159C	2	
5to	SSTMI	00096bba3f0d	IMBAQUINGO C.ROSA M.	Soporte Técnico y Mantenimiento	Sistemas y Telecomunicaciones	SW151C	15	
6to	055-cge-user007	000bcd5e687e		Contraloría General del Estado	Contraloría General del Estado	SW161D	8	

Piso	Nombre de la Computadora	MAC Address	Usuario	Departamento	Unidad	Switch	Puerto	Observación
6to	CTR98-2	0004.acc5.c543		Contraloría General del Estado	Contraloría General del Estado	SW189C	16	Retirada
6to	CTRCR	0004.7621.709d		Contraloría General del Estado	Contraloría General del Estado	SW161D	4	
6to	CTRLP1	000802490202		Contraloría General del Estado	Contraloría General del Estado	SW161D	6	
6to	CTRMV1	0010a41410b4		Contraloría General del Estado	Contraloría General del Estado	SW161D	7	
6to	VCPCO	00096bba3efd	ORDOÑEZ R.CARLOS M.	Vicepresidencia	Vicepresidencia	SW152C	7	
6to	VCPGL	00096b6f7cb7	LEON GONZALO	Vicepresidencia	Vicepresidencia	SW151C	17	
6to	VCPLC	0002553b8db7	CARPIO LEONARDO	Vicepresidencia	Vicepresidencia	SW151C	7	
6to	VCPMP	0002553b8a9f		Vicepresidencia	Vicepresidencia	SW151C	12	
6to	VCPNS	00096b6f7da8	YANEZ G.JORGE A.	Vicepresidencia	Vicepresidencia	SW161D	5	
6to	VCPPO	00096bba3336	OJEDA PATRICIA	Vicepresidencia	Vicepresidencia	SW152C	22	
6to	VCPSM	00096b6f7d0d	MOYANO SILVANIA	Vicepresidencia	Vicepresidencia	SW151C	14	
6to	VCPSN1	00061bc4392d	NEVARES SUCRE	Vicepresidencia	Vicepresidencia	SW151C	23	
7mo	AADJG	00096bba3827	GARZON C.JORGE H.	Administrativa	Administrativa	SW181C	9	
7mo	AADSB	00e0.7d86.0c9c		Administrativa	Administrativa			Desconectada
7mo	AADVI	0004ac537565	IÑIGA VERONICA	Administrativa	Administrativa	SW181C	8	
7mo	DSAEC	0002a5355746	CUEVA Z.EMILIO R.	Servicios Administrativos	Administrativa	SW181C	24	
7mo	DSAFA	0002a536a670	ARAUJO FAUSTO	Servicios Administrativos	Administrativa	SW189C	8	
7mo	DSAFR	0002a536caf9	ROSERO FRANCISCO	Servicios Administrativos	Administrativa	SW189C	18	
7mo	DSAGM	00096bba3402	MOSCOSO S.GUSTAVO E.	Servicios Administrativos	Administrativa	SW181C	4	
7mo	DSAIG	0002a536a5c8	GUERRON IRINA	Servicios Administrativos	Administrativa	SW181C	23	
7mo	DSALL	0002553b8ef9	LUNA LESTER	Servicios Administrativos	Administrativa	SW181C	11	
7mo	DSAPL	0002a52725eb	LUNA PACO	Servicios Administrativos	Administrativa	SW181C	19	
7mo	DSAWC	00096bba3eeb	CALVOPIÑA N.WASHINGTON I.	Servicios Administrativos	Administrativa	SW189C	7	
7mo	SRTBC	00061bde22ba	CORONEL BELEN	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW171C	14	
7mo	SRTJG	0002.555d.a87c	GUALLI C.JUAN C.	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW171C	22	172.20.69.122
7mo	GSTAB1	000d9d5d98f6	BURBANO A.ALBERTO W.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW171C	23	
7mo	GSTAZ	00096bba378b	ZIRITT R.ANA M.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW181C	12	
7mo	GSTCO	0002553b898f	ORDOÑEZ R.CARLOS M.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW189C	24	
7mo	GSTEH	00096bba3409	HERRERA Y.EDGAR L.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW181C	22	
7mo	GSTHC	0002555db0b0	CARPIO T.HECTOR A.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW181C	2	
7mo	GSTPO1	00d0.592e.50fe	ORTIZ PAMELA	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento			Desconectada
7mo	GSTSF	00096bba33e2	FLORES B.SYLVIA E.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW181C	6	
7mo	GSTSL	0002a536a6ed		Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW171C	16	
8vo	DRHAG	0002a5277fac	GUAMANGALLO P.IMELDA A.	Recursos Humanos	Administrativa	SW189C	1	
8vo	DRHCG	00096bba4515	GUERRA G.CINTHYA L.	Recursos Humanos	Administrativa	SW182I	14	
8vo	DRHKP	00096bba32f1	PEÑAFIEL C.KARINA M.	Recursos Humanos	Administrativa	SW181C	20	
8vo	DRHLQ	0002a536a708	QUILLUPANGUI Q.LUIS E.	Recursos Humanos	Administrativa	SW183I	4	
8vo	DRHLS	0002555dbabd	SALGADO M.LUIS F.	Recursos Humanos	Administrativa	SW181C	3	
8vo	DRHPM	0002553b8d47	MANOSALVAS R.PABLO F.	Recursos Humanos	Administrativa	SW183I	3	
8vo	DRHTJ1	00080d975105	JARAMILLO Y.TATHYANA V.	Recursos Humanos	Administrativa	SW181C	18	
8vo	DRHVS	00096bba33ef	SALAZAR L.VICENTE N.	Recursos Humanos	Administrativa	SW183I	1	
8vo	FCOAL	0007e9840052	LIVIAPOMA ANTONIO	Contabilidad	Finanzas	SW182I	16	
8vo	FCOBN	0002a536a67c	NOGALES C.BEATRIZ E.	Contabilidad	Finanzas	SW182I	4	
8vo	FCOCC	0002555dc061	CARRILLO CECILIA	Contabilidad	Finanzas	SW189C	23	
8vo	FCODB	00096bba32c4	BRAVO C.DANILO R.	Contabilidad	Finanzas	SW189C	21	
8vo	FCODI	0002a552dead	IGLESIAS DEYSI	Contabilidad	Finanzas	SW182I	17	
8vo	FCOEP	00096bba3834	PAEZ C.MIGUEL E.	Contabilidad	Finanzas	SW181C	1	
8vo	FCOFH	0002555db5b5	HIDALGO V. FRANCISCO	Contabilidad	Finanzas	SW182I	21	
8vo	FCOGC	00105aa48d37	CADENA GUADALUPE	Contabilidad	Finanzas	SW181C	13	
8vo	FCOLM	00e07d860c9b	MERLO LORENA	Contabilidad	Finanzas	SW129C	13	
8vo	FCOMA	0002a536a656	AYALA P.MARIA M.	Contabilidad	Finanzas	SW182I	23	
8vo	FCOMG	00e07d86350b	GALARRAGA L.MARIO E.	Contabilidad	Finanzas	SW182I	24	
8vo	FCONJ	0007e9840402	JIMENEZ NIXON	Contabilidad	Finanzas	SW182I	5	
8vo	FCONR	00096bba32c5	RAMON L.NANCY C.	Contabilidad	Finanzas	SW182I	12	
8vo	FCONT	00096bba338a	TAPIA R.NELSON A.	Contabilidad	Finanzas	SW181C	10	
8vo	FCOVR	0004ac532602	RAMON C.VIRGINIA E.	Contabilidad	Finanzas	SW182I	10	
8vo	GSAJG	00096bba4027	GALLARDO V. JENNY S.	Subgerencia de Administración y Finanzas	Subgerencia de Administración y Finanzas	SW189C	20	
8vo	GSAMR1	00d0592e51f9	RUIZ E.MARIA E.	Subgerencia de Administración y Finanzas	Subgerencia de Administración y Finanzas	SW189C	15	
9no	DSFEC	00096bba5280	CARVAJAL T.ELIZABETH	Seguridad Física	Administrativa	SW191T	5	
9no	DSFHG	00096b6f74a5	GARZON HERNAN	Seguridad Física	Administrativa	SW181C	5	
9no	DSFOT	0002555db9ac	TAMAYO C.HORACIO R.	Seguridad Física	Administrativa	SW191T	3	
9no	GCCRC	0002555db075	CHAUVIN R.RUTH S.	Legal Gerencia Norte	Legal Gerencia Norte	SW232C	10	
9no	GLEAL	00e04c7ebe37	ABRAHAM E.LOPEZ S	Legal Gerencia Norte	Legal Gerencia Norte	SW191C	6	
9no	GLEALS	0004ac5324e7	LOPEZ ABRAHAM	Legal Gerencia Norte	Legal Gerencia Norte	SW191C	12	
9no	GLEAP	00096bba3812	POZO L. ANA L.	Legal Gerencia Norte	Legal Gerencia Norte	SW191C	5	

Piso	Nombre de la Computadora	MAC Address	Usuario	Departamento	Unidad	Switch	Puerto	Observación
9no	GLEFM	00096bba402c	MACIAS FREDY	Legal Gerencia Norte	Legal Gerencia Norte	SW181C	15	
9no	GLEGD	00096bba3806	DAVALOS C.GIL R.	Legal Gerencia Norte	Legal Gerencia Norte	SW191C	3	
9no	GLEIC	00096b6f7b59	CHAVEZ F.INES M.	Legal Gerencia Norte	Legal Gerencia Norte	SW181C	14	
9no	GLEJV	00096bba3bd7	VELASCO M.JOSE A.	Legal Gerencia Norte	Legal Gerencia Norte	SW182I	22	
9no	GLESF	0002555dbe9a	FERNANDEZ SANTIAGO	Legal Gerencia Norte	Legal Gerencia Norte	SW191C	11	
9no	GLEVM	00096bba3473	MOSQUERA C.VLADIMIR A.	Legal Gerencia Norte	Legal Gerencia Norte	SW189C	5	
9no	GLEHG	00096bba3399		Legal Gerencia Norte	Legal Gerencia Norte	SW191C	1	
9no	LPRJN	00096bba33ea	NIETO F.JOSE S.	Procesos	Legal Gerencia Norte	SW191C	9	
9no	LPRLC	00096bba32f6	CASTRO C.LEONARDO C.	Procesos	Legal Gerencia Norte	SW191T	2	
9no	LPRLT	0004ac537539	TORRES S.LUIS J.	Procesos	Legal Gerencia Norte	SW191C	2	
9no	LPRPC	00e07d860c91	CADENA PATRICIA	Procesos	Legal Gerencia Norte	SW191C	8	
Ex 1er	DBLCA	00096bba32f9	ALVAREZ H.CONSUELO E.	Bienestar Laboral	Administrativa	SW231C	11	
Ex 1er	DBLJL	0002a536a74d	LIMA Z.JENY H.	Bienestar Laboral	Administrativa	SW232C	6	
Ex 1er	GCCAC	00096bba340a	CALDERON S.ALVARO R.	Coordinación de Contratos	Gerencia Regional Norte	SW232C	8	
Ex 1er	GCCHS	00096bba32e0	SALAZAR E.HILDA G.	Coordinación de Contratos	Gerencia Regional Norte	SW232C	9	
Ex 1er	GCCLP	00096bba3b43	PAEZ R. LILIANA DE L.	Coordinación de Contratos	Gerencia Regional Norte	SW231C	14	
Ex 1er	GCCMQ	000629520517		Coordinación de Contratos	Gerencia Regional Norte	SW231C	8	
Ex 1er	GCCOG	00096bba32a5	GARCIA OSWALD	Coordinación de Contratos	Gerencia Regional Norte	SW231C	13	
Ex 1er	GCCTO	00096bba34d4	ORTIZ G.TATIANA M.	Coordinación de Contratos	Gerencia Regional Norte	SW231C	6	
Ex 1er	GCCWG	00096bba3302	GUERRA. C. WILMA. N	Coordinación de Contratos	Gerencia Regional Norte	SW231C	12	172.20.65.220
Ex 1er	GCCXE	0009.6bba.36e6	ESPINOZA A.XIMENA S.	Coordinación de Contratos	Gerencia Regional Norte	SW232C	7	172.20.64.45
Ex 1er	PEPCF	00096bba3306	FRUTOS C.CARLOS A.	Ejecución de Proyectos	Proyectos	SW221C	19	
Ex 1er	PEPFE	00096bba36e4	ESPINEL B.FRANCISCO A.	Ejecución de Proyectos	Proyectos	SW221C	7	
Ex 1er	PEPLB	0002555dba12	BARRERA M.LUIS G.	Ejecución de Proyectos	Proyectos	SW221C	3	
Ex 1er	PEPSQ	00096bba3311	QUISHPE F.SANTIAGO S.	Ejecución de Proyectos	Proyectos	SW221C	16	
Ex 1er	PEPWR	00096bba32f8	REVELO R.WASHINGTON F.	Ejecución de Proyectos	Proyectos	SW221C	5	
Ex 1er	PEVLA	0002a536ec7f	ALDANA B.LINA M.	Evaluación de Proyectos	Proyectos	SW221C	10	
Ex 1er	PEVNS	0002553b89aa	SALAZAR V.NESTOR G.	Evaluación de Proyectos	Proyectos	SW221C	21	
Ex 2do	GCGFE	0002.a536.a5e7	EGUEZ L.FERNANDO R.	Control de Gestión	Gerencia Regional Norte	SW231C	18	172.20.64.39
Ex 2do	GCGIV	0002a536ecac	VELASTEGUI .A INES V.	Control de Gestión	Gerencia Regional Norte	SW231C	24	
Ex 2do	VCGES	0002.555d.b330	SOSA H.LUCIO E.	Control de Gestión	Vicepresidencia	SW231C	3	172.20.64.47
Ex 2do	VCGFNR	00d0592e5030	NARVAEZ R. FRANCISCO	Control de Gestión	Vicepresidencia	SW231C	5	
Ex 2do	VCGFV	0002555db87b	VALDIVIESO O.FAUSTO G.	Control de Gestión	Vicepresidencia	SW231C	4	
Ex 2do	VCGLC	0002555dbe45	CARPIO M.LEONARDO R.	Control de Gestión	Vicepresidencia	SW231C	15	
Ex 2do	VCGLL	0002556b6208	LUZCANDO G.LUIS E.	Control de Gestión	Vicepresidencia	SW232C	2	
Ex 2do	VCGLV	0002a552e978	VASQUEZ LUIS	Control de Gestión	Vicepresidencia	SW232C	23	
Ex 2do	VCGMV	00e07d860c90	VERGARA O.MARIANA DE J.	Control de Gestión	Vicepresidencia	SW231C	1	
Ex 2do	VRPRD	00096bba34ba	DASTE F.RAUL S.	Relaciones Públicas	Vicepresidencia	SW232C	5	
Ex 2do	VRPSV	0002555dabb3	VASCONEZ SUSANA	Relaciones Públicas	Vicepresidencia	SW232C	3	
Ex PB	FJE1	0002a5e00007		Fondo de Jubilación Especial	Fondo de Jubilación Especial	SW201T	2	
Ex PB	FJE2	00e04c8ac542		Fondo de Jubilación Especial	Fondo de Jubilación Especial	SW201T	5	
Ex PB	FJE3	00e04c8ac543		Fondo de Jubilación Especial	Fondo de Jubilación Especial	SW201T	7	
Ex PB	FJE4	0002a5d45a07		Fondo de Jubilación Especial	Fondo de Jubilación Especial	SW201T	1	
Ex PB	FJE5	0002a5cc6b7a		Fondo de Jubilación Especial	Fondo de Jubilación Especial	SW201T	6	
Ex PB	FJESERVER	0002a5ea59ed		Fondo de Jubilación Especial	Fondo de Jubilación Especial	SW201T	3	
Ex PB	PEPAL	00096bba3381	LOPEZ M.JUAN A.	Ejecución de Proyectos	Proyectos	SW221C	11	
Ex PB	PEPCR	00096bba327a	RAMIREZ C.CARLOS O.	Ejecución de Proyectos	Proyectos	SW221C	9	
Ex PB	PEVGC	00096bba3bc6	CUEVA M.GUILLERMO	Evaluación de Proyectos	Proyectos	SW221C	23	
Ex PB	PEVVH	0002555dbcbb	HARO V. VICTORIA	Evaluación de Proyectos	Proyectos	SW221C	8	
Ex PB	GPRFR1	00d0592e4e1c		Proyectos	Proyectos	SW221C	12	
Ex PB	GPRLA	00096bba4001	ARIAS P.LEONI G.	Proyectos	Proyectos	SW221C	6	
Ex PB	GPRMV	0050ba7918a1		Proyectos	Proyectos			Desconectada
Ex PB	SSTJR	00096bba4012	RODRIGUEZ M.JORGE W.	Soporte Técnico y Mantenimiento	Sistemas y Telecomunicaciones	SW221C	20	
Ex PB	SSTPR	00105aa49962		Soporte Técnico y Mantenimiento	Sistemas y Telecomunicaciones	SW202T		
Ex PB	SSTPY	0002555d1255	RODRIGUEZ M.JORGE W.	Soporte Técnico y Mantenimiento	Sistemas y Telecomunicaciones	SW202T		
Ex PB	SSTRC	00096bba338f	CUEVA C.ROXANA S.	Soporte Técnico y Mantenimiento	Sistemas y Telecomunicaciones	SW154C	7	
PB	DSGHL	00096bba3b97	LASSO HENRY	Secretaría General	Administrativa	SW101C	15	
PB	DSGHQ	0004ac536802	QUIROZ HUGO	Secretaría General	Administrativa	SW102I	13	
PB	DSGJB	00096bba3769	BARRIONUEVO JORGE	Secretaría General	Administrativa	SW101C	6	
PB	DSGSM	08005aca9fd8	MOYA F.SILVIA E.	Secretaría General	Administrativa	SW101C	23	
PB	DSAVL	00e0.2936.a4d8	LOPEZ VERONICA	Servicios Administrativos (Recepción Rocio)	Administrativa	SW171C	2	
PB	FAACG1	000bcd5f49d8	GUTIERREZ B.CIRO L.	Administración de Activos	Finanzas	SW101C	14	
PB	FAAJA	00096bba3bf5	ASANZA R.JORGE E.	Administración de Activos	Finanzas	SW101C	7	
PB	FAAJT	0002553b91e6	TIRADO M. JAIME E	Administración de Activos	Finanzas	SW121C	18	
PB	FAASC	00096bba340c	CARPIO SANDRA	Administración de Activos	Finanzas	SW101C	24	

Piso	Nombre de la Computadora	MAC Address	Usuario	Departamento	Unidad	Switch	Puerto	Observación
PB	FAAVC	00105aa499ee	CHERREZ VERONICA	Administración de Activos	Finanzas	SW102I	21	
PB	FAFCT	000d9d4a0b9e	TORRES M.CAMILO V.	Administración Financiera	Finanzas	SW121C	10	
PB	FAFEC	0004ac532452	CAMPOVERDE GOMEZ ELENA	Administración Financiera	Finanzas	SW102I	1	
PB	FAFJB	00096bba333d	BARREIRO V.JORGE A.	Administración Financiera	Finanzas	SW101C	1	
PB	FAFMY	00096bba3333	YEPEZ MARTHA	Administración Financiera	Finanzas	SW122C	2	
PB	FAFNR	00e07d863503	LIBRE	Administración Financiera	Finanzas	SW102I	5	
PB	FAFRS	00096b846fab	SUASNAVAS B.RITA R.	Administración Financiera	Finanzas	SW102I	4	
PB	FAFRV	00096b6f7d3f	VILLACIS H.RAUL E.	Administración Financiera	Finanzas	SW102I	8	
PB	FAFSM	00096bba3bc1	MOREJON SINUHE	Administración Financiera	Finanzas	SW102I	22	
PB	FAFSN	00096bba33dd	NAVARRETE SANDRA	Administración Financiera	Finanzas	SW102I	6	
PB	FCPCC	0002a536a6ff	CASTILLO Y. CARLOS A.	Cuentas por Pagar	Finanzas	SW102I	16	
PB	FCPMG	00096bba3b8e	GALARRAGA L.MARIO E.	Cuentas por Pagar	Finanzas	SW101C	3	
PB	FCPOO	0004ac53758d	OBANDO G.OLGA P.	Cuentas por Pagar	Finanzas	SW122C	4	
PB	FCPPA	00096bba333e	PAULINA AGUIRRE	Cuentas por Pagar	Finanzas	SW102I	18	
Sub	DSABS	00e07d863513	SALTOS BYRON	Servicios Administrativos	Administrativa	SW102I	9	
Sub	DSAGL1	001060767e05	LOPEZ GUILLERMO	Servicios Administrativos	Administrativa	SW101C	20	
Sub	CPECO	0008a1586211	CUCHALA VIVIANA	Cajita de PCO	Cajita de PCO	SW102I	24	

ANEXO 4: Teléfonos IP de la Red la Matriz

TELEFONOS IP DE LA RED LA MATRIZ									
Tipo	MAC Teléfono IP	Usuario	Departamento	Unidad	Switch	Puerto	Nonbre de la Computadora	MAC Address de la Computadora	Observación
TEL & IMP	0800.0f0e.b2e3		Abastecedora	Abastecedora	SW121C	17	Impresora Lexmark T522	000400ec935d	
TEL & PC	0800.0f0e.9abd	AGUAS M.AMPARO DEL C.	Abastecedora	Abastecedora	SW122C	6	CABAA	00096bba3408	
TEL & PC	0800.0f0e.648c	SOLANO C. PETRONIO I.	Coordinación Operativa	Abastecedora	SW122C	20	BCOPS	0002a536a76c	
TEL & PC	0800.0f0e.672b	GARCIA O. JOSE R.	Coordinación Operativa	Abastecedora	SW121C	6	BCOJG	00096b6f7a06	
TEL & PC	0800.0f0e.747e	VELASQUEZ C.GALO E.	Coordinación Operativa	Abastecedora	SW122C	13	BCOGV	0002a536ec7b	
TEL & PC	0800.0f0e.7485	GUERRERO G. LENIN G.	Coordinación Operativa	Abastecedora	SW122C	5	BCOLG	0002a536ec26	
TEL & PC	0800.0f0e.7acd	TOLEDO M.XIMENA DEL R.	Facturación y Ventas	Abastecedora	SW122C	1	BFVXT	0004ac5375d3	
TEL & PC	0800.0f0e.9365	ARIAS A.CARLOS P.	Facturación y Ventas	Abastecedora	SW122C	18	BFVCA	0002553b89b3	
TEL & PC	0800.0f0e.b28f	ZAMBONINO M.VICTOR H.	Facturación y Ventas	Abastecedora	SW121C	9	BFVVZ	0002a536ec84	
TEL & PC	0800.0f0e.73d6	RAMIREZ G.RAUL R.	Liquidación y Consolidación de Cuentas	Abastecedora	SW122C	3	BLCRR	00096b6f7cd3	
TEL & PC	0800.0f07.159b	GARZON C.JORGE H.	Administrativa	Administrativa	SW181C	9	AADJG	00096bba3827	
TEL & PC	0800.0f0e.937e	IÑIGA VERONICA	Administrativa	Administrativa	SW181C	8	AADVI	0004ac537565	
TEL & PC	0800.0f0e.745f	ALVAREZ H.CONSUELO E.	Bienestar Laboral	Administrativa	SW231C	11	DBLCA	00096bba32f9	
TEL & PC	0800.0f0e.6615	GUAMANGALLO P.IMELDA A.	Recursos Humanos	Administrativa	SW189C	1	DRHAG	0002a5277fac	
TEL & PC	0800.0f0e.66a6	SALGADO M.LUIS F.	Recursos Humanos	Administrativa	SW181C	3	DRHLS	0002555dbabd	
TEL & PC	0800.0f0e.73da	JARAMILLO Y.TATHYANA V.	Recursos Humanos	Administrativa	SW181C	18	DRHTJ1	00080d975105	
TEL & PC	0800.0f0e.743e	PEÑAFIEL C.KARINA M.	Recursos Humanos	Administrativa	SW181C	20	DRHKP	00096bba32f1	
TEL & PC	0800.0f0e.b2c9	CARVAJAL T.ELIZABETH	Seguridad Física	Administrativa	SW191T	5	DSFEC	00096bba5280	
TEL & PC	0800.0f0e.65c6	CUEVA Z.EMILIO R.	Servicios Administrativos	Administrativa	SW181C	24	DSAEC	0002a5355746	
TEL & PC	0800.0f0e.6891	GUERRON IRINA	Servicios Administrativos	Administrativa	SW181C	23	DSAIG	0002a536a5c8	
TEL & PC	0800.0f0e.72e8	MOSCOSO S.GUSTAVO E.	Servicios Administrativos	Administrativa	SW181C	4	DSAGM	00096bba3402	
TEL & PC	0800.0f0e.9ab4	LUNA PACO	Servicios Administrativos	Administrativa	SW181C	19	DSAPL	0002a52725eb	
TEL & PC	0800.0f0e.67b5	TOBAR JISELA	Administración de Negocios Propios	Comercializadora	SW129C	23	KANJT	00096bba3313	
TEL & PC	0800.0f01.b773	PADILLA V.AMPARO	Comercializadora	Comercializadora	SW131T	2	CKOEP	00096bba4152	
TEL & PC	0800.0f0e.7767	AGAMA GERMAN	Comercializadora	Comercializadora	SW153C	11	CKOGA	0002a536a71b	
TEL & PC	0800.0f0e.97c1	MESIAS SORAYA	Comercializadora	Comercializadora	SW153C	16	CKOSM	0002555da93c	
TEL & PC	0800.0f0e.92f7	YONFA C.SANDRA J.	Coordinación Operativa y Ventas	Comercializadora	SW131T	3	KCOSY	0002a536a6ca	
TEL & PC	0800.0f0e.995e	ARGUELLO A.ESTEBAN R.	Coordinación Operativa y Ventas	Comercializadora	SW153C	12	KCOEA	0002555db06b	
TEL & PC	0800.0f0e.9387	SAUD FERNANDO	Mercadeo y Atención al Cliente	Comercializadora	SW151C	3	KMAFS	0002553b866d	
TEL & PC	0800.0f0e.63ab	ESPINOZA A.XIMENA S.	Coordinación de Contratos	Coordinación de Contratos	SW232C	7	GCCXE	0009.6bba.36e6	
TEL & PC	0800.0f0e.6514	GARCIA OSWALD	Coordinación de Contratos	Coordinación de Contratos	SW231C	13	GCCOG	00096bba32a5	
TEL & PC	0800.0f0e.68a8	ORTIZ G.TATIANA M.	Coordinación de Contratos	Coordinación de Contratos	SW231C	6	GCCTO	00096bba34d4	
TEL & PC	0800.0f0e.73d1	GUERRA. C. WILMA. N	Coordinación de Contratos	Coordinación de Contratos	SW231C	12	GCCWG	00096bba3302	
TEL & PC	0800.0f0e.995d		Coordinación de Contratos	Coordinación de Contratos	SW231C	8	GCCMQ	000629520517	
TEL & PC	0800.0f0e.99e9	CALDERON S.ALVARO R.	Coordinación de Contratos	Coordinación de Contratos	SW232C	8	GCCAC	00096bba340a	
TEL & PC	0800.0f0e.6875	GUTIERREZ B.CIRO L.	Administración de Activos	Finanzas	SW101C	14	FAACG1	000bcd5f49d8	
TEL & PC	0800.0f0e.68bf	ASANZA R.JORGE E.	Administración de Activos	Finanzas	SW101C	7	FAAJA	00096bba3bf5	
TEL & PC	0800.0f0e.676b	MOREJON SINUHE	Administración Financiera	Finanzas	SW102I	22	FAFSM	00096bba3bc1	
TEL & PC	0800.0f0e.84c1	BARREIRO V.JORGE A.	Administración Financiera	Finanzas	SW101C	1	FAFJB	00096bba333d	
TEL & PC	0800.0f0e.954a	TORRES M.CAMILO V.	Administración Financiera	Finanzas	SW121C	10	FAFCT	000d9d4a0b9e	
TEL & PC	0800.0f0e.b26e	YEPEZ MARTHA	Administración Financiera	Finanzas	SW122C	2	FAFMY	00096bba3333	
TEL & PC	0800.0f0e.67ad	PAEZ C.MIGUEL E.	Contabilidad	Finanzas	SW181C	1	FCOEP	00096bba3834	
TEL & PC	0800.0f0e.778a	NOGALES C.BEATRIZ E.	Contabilidad	Finanzas	SW182I	4	FCOBN	0002a536a67c	
TEL & PC	0800.0f0e.7b41	CADENA GUADALUPE	Contabilidad	Finanzas	SW181C	13	FC0GC	00105aa48d37	
TEL & PC	0800.0f0e.b0db	TAPIA R.NELSON A.	Contabilidad	Finanzas	SW181C	10	FCONT	00096bba338a	
TEL & PC	0800.0f0e.b0de	DAVILA ERIKA	Crédito y Cobranzas	Finanzas	SW122C	14	FCCED	0002a536e7f9	
TEL & PC	0800.0f0e.0618	GALARRAGA L.MARIO E.	Cuentas por Pagar	Finanzas	SW101C	3	FCPMG	00096bba3b8e	
TEL & PC	0800.0f0e.92b9	OBANDO G.OLGA P.	Cuentas por Pagar	Finanzas	SW122C	4	FCPOO	0004ac53758d	
TEL & PC	0800.0f0e.6697	ARTIEDA CARLOS	Presupuesto	Finanzas	SW122C	16	AFICA	000d606b6281	
TEL & PC	0800.0f0e.b2de	GARCIA INES	Presupuesto	Finanzas	SW121C	7	FPRIG	0002553b83b2	
TEL & PC	0800.0f0e.9752	BURBANO PATRICIA	Seguros y garantías	Finanzas	SW121C	13	FSGPB	0002a556ab3c	
TEL & PC	0800.0f0e.b0dd	TAPIA M.MARGARITA E.	Seguros y garantías	Finanzas	SW121C	11	FSGMT	0004.ac53.787d	
TEL & PC	0800.0f0e.652c	EGUEZ L.FERNANDO R.	Control de Gestión	Gerencia Regional Norte	SW231C	18	GCGFE	0002.a536.a5e7	
TEL & PC	0800.0f0e.746b	VELASTEGUI .A INES V.	Control de Gestión	Gerencia Regional Norte	SW231C	24	GCGIV	0002a536ecac	
TEL & PC	0800.0f04.dd70	POZO L. ANA L.	Legal Gerencia Norte	Legal Gerencia Norte	SW191C	5	GLEAP	00096bba3812	
TEL & PC	0800.0f0e.92a4	FERNANDEZ SANTIAGO	Legal Gerencia Norte	Legal Gerencia Norte	SW191C	11	GLESF	0002555dbe9a	
TEL & PC	0800.0f0e.92a9	MACIAS FREDY	Legal Gerencia Norte	Legal Gerencia Norte	SW181C	15	GLEFM	00096bba402c	
TEL & PC	0800.0f0e.92fb	TORRES P.GUSTAVO J.	Compras Locales	Materiales	SW122C	19	MCLGT	0002a536ebff	
TEL & PC	0800.0f0e.b2b0	GALLARDO T.MIRIAM S.	Control de Materiales y Bodega	Materiales	SW122C	17	MCMMG	0002a536eca9	
TEL & PC	0800.0f0e.65d6	PAZMIÑO P.SILVIA M.	Importaciones	Materiales	SW121C	21	MIMSP	00096bba327b	
TEL & PC	0800.0f0e.667c	RAMIREZ C.CARLOS O.	Ejecución de Proyectos	Proyectos	SW221C	9	PETEL & PCR	00096bba327a	
TEL & PC	0800.0f0e.97c0	LOPEZ M.JUAN A.	Ejecución de Proyectos	Proyectos	SW221C	11	PEPAL	00096bba3381	
TEL & PC	0800.0f0e.7476	HARO V. VICTORIA	Evaluación de Proyectos	Proyectos	SW221C	8	PEVVH	0002555dbcbb	
TEL & PC	0800.0f0e.9389	ALDANA B.LINA M.	Evaluación de Proyectos	Proyectos	SW221C	10	PEVLA	0002a536ec7f	
TEL & PC	0800.0f0e.b22c		Proyectos	Proyectos	SW221C	12	GPRFR1	00d0592e4e1c	
TEL & PC	0800.0f0e.9ab8	CANGAHUAMIN J.MAYRA P.	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW152C	10	SIPMC	00096bba3390	
TEL & PC	0800.0f10.26e6	QUILCA LUIS	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW151C	4	SIPLQ	0002555db078	

Tipo	MAC Teléfono IP	Usuario	Departamento	Unidad	Switch	Puerto	Nonbre de la Computadora	MAC Address de la Computadora	Observación
TEL & PC	0800.0f10.27b9	ROMERO V.ROSA M.	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW152C	5	SIPRR	00096bba3382	
TEL & PC	0800.0f0f.ab30	PAEZ GUSTAVO	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW151C	19	SRTCP	00096bba3383	
TEL & PC	0800.0f10.2c98	CORONEL BELEN	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW171C	14	SRTBC	00061bde22ba	
TEL & PC	0800.0f0e.9330	SALINAS H. JAQUELINE M.	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW152C	2	GSIJS	00096b90b709	
TEL & PC	0800.0f0e.93a8	MANCHENO O.GUILLERMO O.	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW153C	8	GSIGM	00096bba3bc3	
TEL & PC	0800.0f10.27d3	LARA F.SANDRA M.	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW152C	9	GSISL	00096bba33ab	
TEL & PC	0800.0f04.fef3	RIVERA S.BLANCA M.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	16	SSABR	000d.606a.f7cd	
TEL & PC	0800.0f0e.66fa	GALLO L.ROBERTH F.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW152C	14	SSARG	000d606b5a16	
TEL & PC	0800.0f0e.7733	DELGADO G.JOSE J.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	19	SSAJD	000d606b62d5	
TEL & PC	0800.0f0e.77c6	MURILLO C.JIMMY HECTOR V.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW152C	21	SSAJM	00096bba377e	
TEL & PC	0800.0f0e.d412	GRIJALVA R.LUIS F.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	1	SSALG	00096bba34c7	
TEL & PC	0800.0f10.275c	VILLACIS M.JENNY L.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	3	SSAJV	0002555dc0a5	
TEL & PC	0800.0f10.2a6f	VILLAVICENCIO G.LUIS O.	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW151C	8	SSALOV	00096bba3316	
TEL & PC	0800.0f0e.9550	IMBAQUINGO C.ROSA M.	Soporte Técnico y Mantenimiento	Sistemas y Telecomunicaciones	SW151C	15	SSTMI	00096bba3f0d	
TEL & PC	0800.0f0e.66ee	RUIZ E.MARIA E.	Subgerencia de Administración y Finanzas	Subgerencia de Administración y Finanzas	SW189C	15	GSAMR1	00d0592e51f9	
TEL & PC	0800.0f0e.6729	GALLARDO V. JENNY S.	Subgerencia de Administración y Finanzas	Subgerencia de Administración y Finanzas	SW189C	20	GSAJG	00096bba4027	
TEL & PC	0800.0f0e.6876	CEVALLOS M.HILDA P.	Subgerencia de Comercialización	Subgerencia de Comercialización	SW153C	22	GSCHC	00096bba3831	
TEL & PC	0800.0f0e.7791	DURANGO L. MARTHA C.	Subgerencia de Comercialización	Subgerencia de Comercialización	SW152C	4	GSCMD	0002553b8792	
TEL & PC	0800.0f01.b767	BURBANO A.ALBERTO W.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW171C	23	GSTAB1	000d9d5d98f6	
TEL & PC	0800.0f0e.733a	HERRERA Y.EDGAR L.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW181C	22	GSTEH	00096bba3409	
TEL & PC	0800.0f0e.733c	CARPIO T.HECTOR A.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW181C	2	GSTHC	0002555db0b0	
TEL & PC	0800.0f0e.743d	ZIRITT R.ANA M.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW181C	12	GSTAZ	00096bba378b	
TEL & PC	0800.0f0e.9210		Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW171C	16	GSTSL	0002a536a6ed	
TEL & PC	0800.0f10.8b43	FLORES B.SYLVIA E.	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW181C	6	GSTSF	00096bba33e2	
TEL & PC	0800.0f0e.7463	VERGARA O.MARIANA DE J.	Control de Gestión	Vicepresidencia	SW231C	1	VCGMV	00e07d860c90	
TEL & PC	0800.0f0e.7484	VALDIVIESO O.FAUSTO G.	Control de Gestión	Vicepresidencia	SW231C	4	VCGFV	0002555db87b	
TEL & PC	0800.0f0e.749a	LUZCANDO G.LUIS E.	Control de Gestión	Vicepresidencia	SW232C	2	VCGLL	0002556b6208	
TEL & PC	0800.0f0e.7cae	NARVAEZ R. FRANCISCO	Control de Gestión	Vicepresidencia	SW231C	5	VCGFNR	00d0592e5030	
TEL & PC	0800.0f0e.97c5	SOSA H.LUCIO E.	Control de Gestión	Vicepresidencia	SW231C	3	VCGES	0002.555d.b330	
TEL & PC	0800.0f0e.6734		Gerencia Regional Norte	Vicepresidencia	SW154C	14	VGNJF1	000039863ee9	
TEL & PC	0800.0f0e.74bd		Gerencia Regional Norte	Vicepresidencia	SW122C	9	VGNAC	00055d26c127	
TEL & PC	0800.0f0e.8441	GARCIA S.GIOVANNA E.	Gerencia Regional Norte	Vicepresidencia	SW153C	20	VGNEG	0002a565e400	
TEL & PC	0800.0f0e.97ba	FIALLO C.JAIME G.	Gerencia Regional Norte	Vicepresidencia	SW153C	19	VGNGF	00096bba331e	
TEL & PC	0800.0f0e.9b90	RAMIREZ CARLOS	Gerencia Regional Norte	Vicepresidencia	SW153C	10	VGNCR	0010605b80b8	
TEL & PC	0800.0f0e.93ba	TORRES M.CONSUELO E.	Legal Vicepresidencia	Vicepresidencia	SW153C	15	VLECT	00096bba3bc0	
TEL & PC	0800.0f0e.9386	PAZMIÑO G.DORA M.	Planificación y Finanzas	Vicepresidencia	SW149C	7	VPFDP	00096bba3305	
TEL & PC	0800.0f0e.9748	GUARDERAS FERNANDO	Planificación y Finanzas	Vicepresidencia	SW149C	6	VPFFG	00096bba400a	
TEL & PC	0008.0f0e.938f	ALARCON C.NICOLAS A.	Programación	Vicepresidencia	SW159C	21	VPRNA	00096bba3395	
TEL & PC	0800.0f07.1313	DE LA CRUZ G.MARTHA Z.	Programación	Vicepresidencia	SW151C	10	VPRMC	0002a536ec79	
TEL & PC	0800.0f0e.68ce		Vicepresidencia	Vicepresidencia	SW151C	12	VCPMP	0002553b8a9f	
TEL & PC	0800.0f0e.84c2	DIAZ ALONSO	Vicepresidencia	Vicepresidencia	SW151C	11	VCPAD	0002553b8c7c	
TEL & PC	0800.0f0e.9548	OJEDA PATRICIA	Vicepresidencia	Vicepresidencia	SW152C	22	VCPPO	00096bba3336	
TEL & PC	0800.0f0e.955c	NEVARES SUCRE	Vicepresidencia	Vicepresidencia	SW151C	23	VCPSN1	00061bc4392d	
TEL & PC	0800.0f10.24eb	CARPIO LEONARDO	Vicepresidencia	Vicepresidencia	SW151C	7	VCPLC	0002553b8db7	
TEL & PC	0800.0f10.89d9	ORDOÑEZ R.CARLOS M.	Vicepresidencia	Vicepresidencia	SW152C	7	VCTEL & PCO	00096bba3efd	
TEL & PC	0800.0f10.8bce	MOYANO SILVANIA	Vicepresidencia	Vicepresidencia	SW151C	14	VCPSM	00096b6f7d0d	
TEL	0800.0f0e.75e3		Bienestar Laboral	Administrativa	SW231C	10			
TEL	0800.0f0e.9372		Bienestar Laboral	Administrativa	SW231C	9			
TEL	0800.0f0e.0616		Secretaría General	Administrativa	SW101C	5			
TEL	0800.0f0e.74c3		Servicios Administrativos	Administrativa	SW171C	6			
TEL	0800.0f0e.9392		Servicios Administrativos	Administrativa	SW231C	21			RecepTEL & PCión Exsal
TEL	0800.0f0e.65a2		Administración Financiera	Finanzas	SW122C	15			
TEL	0800.0f10.2759		Administración Financiera	Finanzas	SW101C	9			
TEL	0800.0f0e.97cb		Crédito y Cobranzas	Finanzas	SW121C	5			
TEL	0800.0f0e.933b		Finanzas	Finanzas	SW122C	22			
TEL	0800.0f0e.7b95		Presupuesto	Finanzas	SW121C	1			
TEL	0800.0f0e.75fe		Legal Gerencia Norte	Legal Gerencia Norte	SW181C	16			
TEL	0800.0f0e.74c0		Ejecución de Proyectos	Proyectos	SW221C	17			
TEL	0800.0f0e.65ad		Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW171C	3			
TEL	0800.0f10.2bb4		Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW157T	5			
TEL	0800.0f07.49b7		Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW152C	11			
TEL	0800.0f09.3a26		Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW152C	17			
TEL	0800.0f0e.75eb		Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW181C	17			
TEL	0800.0f10.2641		Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW171C	24			
TEL	0800.0f0e.b217		Relaciones Públicas	Vicepresidencia	SW231C	7			
TEL	0800.0f0e.65fd		Vicepresidencia	Vicepresidencia	SW153C	21			
TEL	0800.0f10.291c		Vicepresidencia	Vicepresidencia	SW151C	13			
TEL	0800.0f10.88a0		Vicepresidencia	Vicepresidencia	SW161D	1			
TEL	0800.0f0d.fb8f				SW232C	15			Especial
TEL	0800.0f0d.dc7c				SW231C	20			No registrado
TEL	0800.0f0e.22a8				SW231C	23			No registrado
TEL	0800.0f0e.22b5				SW231C	19			No registrado

ANEXO 5: Equipos e Impresoras de la Red la Matriz

EQUIPOS E IMPRESORAS DE LA RED LA MATRIZ							
Tipo	**Nombre del Equipo**	**MAC Address**	**Departamento**	**Unidad**	**Switch**	**Puerto**	**Observación**
EQ	DSR-2000 Califur by Kalatel		Seguridad Física	Administrativa	SW191T	1	
EQ	Servidor PCORED5 backup	000d.606b.61ee	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW157T	4	
EQ	Controlador de la Central Telefónica	0800.0f05.0572	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW171C	2	
EQ	Controlador de la Central Telefónica	0800.0f05.18a1	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW171C	2	
EQ	Firewall IBM (vlan1) - LAN interna	0004.ac17.0e32	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW155C	16	
EQ	Firewall IBM (vlan2) - Filiales	0002.55af.1d7e	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW155C	18	
EQ	Firewall IBM (vlan3) - LAN Externa	0004.ac3e.e44e	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW155C	21	
EQ	Router Vanguard (200)		Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW155C	5	
EQ	PCO1 (QPCO1)	727.777.777.777	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW159C	7	
EQ	PCO2 (QS104297M)	727.777.777.707	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW159C	10	
EQ	PCO8 (QS102F6FC)	0009.6b65.0611	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW159C	11	
EQ	PCO9 (QA102F6FC)	0009.6b65.0908	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW159C	3	
EQ	PcoFirewall	00105aa499e9	Ingeniería y Procesamiento	Sistemas y Telecomunicaciones	SW155C	11	Ya no existe
EQ	Router Cisco 800 Series	00b0.c28d.fd8a	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW155C	9	
EQ	Router IBM 2210 (Dial-up)	0004.acca.7458	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW155C	3	
EQ	Router IBM 2210 (Internet y SRI)	0004.acca.17c8	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW155C	22	
EQ	Router IBM 2216-400	0200.0000.8c4e	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW155C	2	
EQ	Servidor PCORED2	0050.8be9.0a7e	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW159C	12	Ya no existe
EQ	Servidor IBM PCORED3	0009.6bba.3320	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW159C	20	Ya no existe
EQ	Servidor PCORED	0050.8be7.fe20	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW155C	7	
EQ	Servidor PCORED1	0060.94b9.bb6e	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW155C	12	
EQ	Servidor PCORED4	0010.b548.d830	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW155C	14	
EQ	Servidor PCORED6	0002.a55c.f574	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW155C	10	Ya no existe
EQ	Servidor PCORED7	0001.03cd.8085	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW154C	18	
EQ	Servidor PCOWEB	0050.8be9.05e0	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW155C	23	
EQ	Switch IBM (SW102I)	0090.04ec.54f8	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW102I		
EQ	Switch IBM (SW111I)	0090.0437.fef8	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW111I		
EQ	Switch IBM (SW141I)	0004.acd9.09c5	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW141I		
EQ	Switch IBM (SW182I)	0090.04ec.5178	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW182I		
EQ	Switch IBM (SW183I)	0090.04ec.53f8	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW183I		
EQ	Switch/Router IBM 8274		Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	SW155C	4	
IMP	Impresora Lexmark Optra S 1650	0004.00c8.dc9c	Abastecedora	Abastecedora	SW129C	22	
IMP	Impresora Lexmark T522	000400ec935d	Abastecedora	Abastecedora	SW121C	17	
IMP	Impresora Lexmark T522	0004.00ec.93f5	Comercializadora	Comercializadora	SW131T	7	
IMP	Impresora Lexmark Optra S 1650	0004.0030.b670	Contabilidad	Finanzas	SW189C	3	
IMP	Impresora Lexmark Optra S 1650	0004.0030.4a27	Coordinación de Contratos	Gerencia Regional Norte	SW231C	16	
IMP	Impresora Lexmark T522	0004.00ec.9325	Legal Gerencia Norte	Legal Gerencia Norte	SW191C	7	
IMP	Impresora Lexmark Optra S 1650	0004.0030.4a0f	Presupuesto	Finanzas	SW129C	4	
IMP	Impresora Lexmark T522	0004.00ec.d31e	Servicios Administrativos	Administrativa	SW182I	8	
IMP	Impresora IBM Infoprint 1145	0004.00e2.7f3f	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW159C	16	
IMP	Impresora IBM Infoprint 1145	0004.00e2.ffae	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW159C	17	
IMP	Impresora Lexmark C720	0004.00ec.d395	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW154C	10	
IMP	Impresora Lexmark T522	0004.00ec.93b5	Sistemas y Telecomunicaciones	Sistemas y Telecomunicaciones	SW152C	15	
IMP	IMPRESORA LEXMARK C720	0004.00ec.d3b5	Soporte de Aplicaciones	Sistemas y Telecomunicaciones	SW141I	2	
IMP	Impresora Lexmark Optra S 1650	00040030ca10	Soporte Técnico y Mantenimiento	Sistemas y Telecomunicaciones	SW202T		
IMP	Impresora HP	0001.e63e.8af6	Subgerencia de Transporte y Almacenamiento	Subgerencia de Transporte y Almacenamiento	SW171C	18	

ANEXO 6: Direcciones IP Actuales de la Red la Matriz

Direcciones IP de la Matriz - Quito Red: 172.20.64.0/21		
Esquema Actual		
Rango	**Detalle**	**Descripción**
64.1 - 64.19 Comunicaciones	.1	Libre
	.2	Router IBM 2216-400 (Corazón, Chalpi)
	.3	Router CISCO 800 Series (Guayaquil, Cuenca, Riobamba)
	.4	Router IBM 2210 Dial up
	.5	Impresora IBM Infoprint 1145 (Sistemas)5to p
	.6	Firewall IBM AIX
	.7	Libre
	.8	Libre
	.9	Impresora IBM Infoprint 1145 (Sistemas)5to p
	.10	Switch/Router IBM 8274 (de baja)
	.11	Router Vanguard Motorola
	.12 - .19	RAS
64.20 - 64.29 AS/400	.20	Pcored
	.21	Libre
	.22	Libre
	.23	Libre
	.24	Pcored4
	.25	Pco1
	.26	Pco2
	.27	Pco4 (no utilizado)
	.28	Pco8
	.29	Pco9
64.30 - 64.49 Direcciones para control del Firewall	.30	Libre
	.31	Soporte de Aplicaciones (SSAFT)
	.32	Impresora Lexmark Optra 1650 (Presupuesto)2do p
	.33	Libre
	.34	Libre
	.35	Libre
	.36	Impresora Lexmark Optra 1650 (Coor. Contratos)Ex_1er p
	.37	Impresora Lexmark Optra 1650 (Mtto. Sistemas)Ex_pb
	.38	Libre
	.39	Control de Gestión (VCGFE)
	.40	Libre
	.41	Seguros y Garantías (FSGMT)
	.42	Seguros y Garantías (FSGMV)
	.43	Libre
	.44	Seguros y Garantías (FSGFG)
	.45	Coordinación de Contratos (GCCXE)
	.46	Coordinación de Contratos (GCCWG)
	.47	Coordinación de Contratos (GCCWG)
	.48	Coordinación de Contratos (GCCWG)
	.49	Libre
64.50 - 64.69 Servidores	.50	Libre
	.51	Libre
	.52	Pcored2 (de baja)
	.53	Pcored3
	.54	Libre
	.55	Pcored5
	.56	Libre
	.57	Pcored7
	.58	Libre
	.59	Libre
	.60	Libre
	.61	Libre
	.62	Libre
	.63	Libre
	.64	Libre
	.65	Libre
	.66	Libre
	.67	Libre
	.68	Libre
	.69	Libre
64.70 - 64.99 Impresoras con tarjeta de red	.70	Impresora 1er piso
	.71	Impresora 1er piso
	.72	Impresora 1er piso
	.73	Impresora 2do piso
	.74	Impresora Lexmark T522 (Abastecedora) 2do p
	.75	Impresora 2do piso
	.76	Impresora Lexmark T522 (Comercializadora) 3er p
	.77	Impresora Lexmark Optra 1650 (Abastecedora) 2do p
	.78	Impresora 3er piso
	.79	Impresora Lexmark C720 (Soporte y Aplicaciones) 4to p
	.80	Impresora 4to piso
	.81	Impresora 4to piso
	.82	Impresora 5to piso
	.83	Impresora Lexmark T522 (Sistemas y Telec.) 5to p
	.84	Impresora Lexmark C720 (Sistemas y Telec.) 5to p
	.85	Impresora Lexmark T522 (Servicios Admin.) 5to p
	.86	Impresora 6to piso
	.87	Impresora 6to piso
	.88	Impresora HP (Subgerencia de Transporte) 7mo p
	.89	Impresora 7mo piso
	.90	Impresora 7mo piso
	.91	Impresora Lexmark Optra 1650 (Contabilidad) 8vo p
	.92	Impresora 8vo piso
	.93	Impresora 8vo piso
	.94	Impresora Lexmark T522 (Legal Gerencia Norte) 9no p
	.95	Impresora 9no piso
	.96	Impresora 9no piso
	.97	Impresora El Rocío II
	.98	Impresora El Rocío II
	.99	Impresora El Rocío II
64.101 - 64.232 Switches Cisco	.101	Switch Cisco Pco_101
	.121	Switch Cisco Pco_121
	.122	Switch Cisco Pco_122
	.129	Switch Cisco Pco_129
	.141	Switch Cisco Pco_141
	.149	Switch Cisco Pco_149
	.151	Switch Cisco Pco_151
	.152	Switch Cisco Pco_152
	.153	Switch Cisco Pco_153
	.154	Switch Cisco Pco_154
	.159	Switch Cisco Pco_159
	.171	Switch Cisco Pco_171
	.181	Switch Cisco Pco_181
	.189	Switch Cisco Pco_189
	.191	Switch Cisco Pco_191
	.221	Switch Cisco Pco_221
	.231	Switch Cisco Pco_231
	.232	Switch Cisco Pco_232
65.1 - 68.254		Direcciones del DHCP para la red de datos
69.1	.1	Controlador de la Central IP Mitel
69.30 - 69.240		Direcciones del DHCP de la Central para la teléfonos IP
69.242	.242	E2T de la Central IP Mitel
71.9	.9	Pcored6 (de baja)
71.21	.21	Pcored1

ANEXO 7 Computadoras y Equipos de la Red de Beaterio

COMPUTADORAS Y EQUIPOS DE LA RED DE BEATERIO							
SW #	Switch	Puerto	Nombre de Maquina	Dirección MAC	Dirección IP	Departamento	Unidad
SW1	SW 3COM (8puertos)	1	Bridge 3COM a Telecomunicaciones				
SW1	SW 3COM (8puertos)	2	QJMCL	00-02-55-5D-B6-41	172.20.129.197	Jet Fuel	Superintendencia de Terminales y Depósitos
SW2	SW 3COM (8puertos)	1	A SW Jefatura de Term. con Transc. DMC				
SW2	SW 3COM (8puertos)	2	BBT74	00-8100-80-A6-9C	172.20.129.64	Bodega	Materiales
SW2	SW 3COM (8puertos)	3	QBB21	00-09-6B-BA-34-04	172.20.129.121	Bodega	Materiales
SW3	SW CISCO 2900XL	1	BSQLM	00-09-6B-BA-32-F2	172.20.129.104	Sucursal Quito (Comercializadora)	Abastecedora
SW3	SW CISCO 2900XL	2	BSQAC	00-08-02-21-9A-B9	172.20.129.69	Sucursal Quito (Comercializadora)	Abastecedora
SW3	SW CISCO 2900XL	3	DMBGM	00-02-A5-36-EC-69	172.20.129.187	Dispensario Médico	
SW3	SW CISCO 2900XL	4	DMOBJM	00-02-A5-36-A7-5C	172.20.129.188	Dispensario Médico	
SW3	SW CISCO 2900XL	5	BSQMB	00-02-55-3B-8D-D4	172.20.129.109	Sucursal Quito (Comercializadora)	Abastecedora
SW3	SW CISCO 2900XL	6	BSQAS	00-04-AC-53-75-A8	172.20.129.107	Sucursal Quito (Comercializadora)	Abastecedora
SW3	SW CISCO 2900XL	7	BSQGC	00-02-A5-36-A6-E9	172.20.129.108	Sucursal Quito (Comercializadora)	Abastecedora
SW3	SW CISCO 2900XL	8	BSQEP	00-09-6B-BA-33-1A	172.20.129.72	Sucursal Quito (Comercializadora)	Abastecedora
SW3	SW CISCO 2900XL	11	A SW Jefatura. con Transc. MC101				
SW3	SW CISCO 2900XL	12	A SW Pol. Q.A.R. con Transc. MC102XL				
SW4	SW CISCO 3500XL	1	MOPRO1	00-10-5A-45-S1-26	172.20.129.106	Mopro	MOPRO
SW4	SW CISCO 3500XL	3	MOPRO2	00-10-5A-A5-F1-26	172.20.129.110	Mopro	MOPRO
SW4	SW CISCO 3500XL	5	YTBAC	00-0802-21-B2-43	172.20.129.101	Produtos Limpios	Superintendencia de Terminales y Depósitos
SW4	SW CISCO 3500XL	11	QJM11	00-02-A5-28-EE-45	172.20.129.111	Jef. Mtto. Terminal	Superintendencia de Terminales y Depósitos
SW4	SW CISCO 3500XL	12	A SW de Ctrl. Calidad				
SW4	SW CISCO 3500XL	13	YTBNV	00-60-94-EA-14-91	172.20.129.105	Produtos Limpios	Superintendencia de Terminales y Depósitos
SW4	SW CISCO 3500XL	14	A SW Comercializadora con Transc. MC101				
SW4	SW CISCO 3500XL	16	A SW Bodega con Transc. DMC				
SW4	SW CISCO 3500XL			00-50-BA-79-DF-3F	172.20.129.248		
SW4	SW CISCO 3500XL	19	TITJG	00-02-A5-27-78-3B	172.20.129.86	Inspección Técnica	Inspección Técnica
SW4	SW CISCO 3500XL	21	TYEES	00-10-5A-86-0C-95	172.20.129.85	Jef. Mtto. Terminal	Superintendencia de Terminales y Depósitos
SW4	SW CISCO 3500 XL	23	TELEFONO		172.20.129.177	Superint. de Terminales	Superintendencia de Terminales y Depósitos
SW5	SW CISCO 3550	1	SRTCS1	00-D0-59-2E-52-24	172.20.129.122	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones
SW5	SW CISCO 3550	3			172.20.129.11	Router 6455 (220)	
SW5	SW CISCO 3550	4			172.20.129.150	Central Telefónica MITEL	
SW5	SW CISCO 3550	5	Bridge 3COM a Jet Fuel				
SW5	SW CISCO 3550	8	SRTJL	00-02-A5-52-E6-45	172.20.129.185	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones
SW5	SW CISCO 3550	11	GSTIA	00-09-6B-E2-0A-DB	172.20.129.186	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones
SW5	SW CISCO 3550	13	STDFC	00-02-55-5D-B4-E1	172.20.129.250	Superint. de Terminales	Superintendencia de Terminales y Depósitos
SW5	SW CISCO 3550	17			172.20.129.165	Jef. Mtto. Terminal	Superintendencia de Terminales y Depósitos
SW5	SW CISCO 3550	23	A SW de Mtto Electrico				
SW5	SW CISCO 3550	24	YMTGJM	00-09-6B-C4-23-83	172.20.129.115	Superint. de Terminales	Superintendencia de Terminales y Depósitos
SW6	SW CNET(8puertos)	1	A SW Pol. Q.A.R.				
SW6	SW CNET (8puertos)	5	EEBEL	00-02-A5-36-A7-33	172.20.129.102	Reductora	Superint. Poliducto Esm-StoDmgo-Quito-Mac
SW6	SW CNET(8puertos)	6			172.20.129.167	Reductora	Superint. Poliducto Esm-StoDmgo-Quito-Mac
SW7	SW CNET (8puertos)	1	A SW Jefatura de Terminal				
SW7	SW CNET (8puertos)	2	Lab1	00-10-B5-72-F0-B5	172.20.129.98	Lab. Control de Calidad	Superintendencia de Terminales y Depósitos
SW7	SW CNET (8puertos)	3	YCCPJ	00-02-55-5D-BA-11	172.20.129.99	Lab. Control de Calidad	Superintendencia de Terminales y Depósitos
SW8	SW DLINK (5puertos)	1	A SW Pol. Q.A.R.				
SW8	SW DLINK(5puertos)		GPIJM (Portatil)	00-0E-7F-7B-E7-B5	172.20.129.196	Protección Ambiental	Protec. Ambiental y Seguridad Industrial
SW8	SW DLINK(5puertos)		GPICS2	XX-XX-XX-49-5F-C7	172.20.129.240	Seguridad Industrial	Protec. Ambiental y Seguridad Industrial
SW8	SW DLINK(5puertos)	4	GPICS	00-02-55-5D-B8-C2	172.20.129.194	Seguridad Industrial	Protec. Ambiental y Seguridad Industrial
SW8	SW DLINK (5puertos)	5	PSI04	00-05-5D-2A-CC-B3	172.20.129.50	Seguridad Industrial	Protec. Ambiental y Seguridad Industrial
SW9	SW DLINK (8puertos)	3	TPQAES	00-09-6B-BA-37-7B	172.20.129.103	Superint. Poliducto Q-A-R	Superint. Poliducto Quito-Ambato-Riobamba
SW9	SW DLINK (8puertos)	4	QOPISI	00-09-6B-BA-32-E8	172.20.129.87	Operaciones P. Q-A-R (Est. Bombeo)	Superint. Poliducto Quito-Ambato-Riobamba
SW9	SW DLINK (8puertos)		QARWJ - (PRESTAMO de TELECOM.)	00-10-60-76-7D-F1	172.20.129.136	Mtto. De Linea de .P Q-A-R	Superint. Poliducto Quito-Ambato-Riobamba
SW9	SW DLINK (8puertos)		TPQMM	00-0D-9D-5D-8E-7D	172.20.129.253	Superint. Poliducto Q-A-R	Superint. Poliducto Quito-Ambato-Riobamba
SW9	SW DLINK (8puertos)	5	A SW Reductora				
SW9	SW DLINK (8puertos)	7	A SW Seguridad Industrial				
SW9	SW DLINK (8puertos)	8	A SW Comercializadora con Transc. MC102XL				
SW10	SW DLINK(8 puertos)	1	A SW de Telecomunicaciones				
SW10	SW DLINK(8puertos)	2			172.20.129.198	Mtto. Eléctrico (Portatil)	Superintendencia de Terminales y Depósitos
SW10	SW DLINK(8puertos)	4	PJC-02	00-02-3F-80-A1-8B	172.20.129.195	Mtto. Eléctrico (Portatil)	Superintendencia de Terminales y Depósitos
SW10	SW DLINK(8 puertos)	8		00-10-5A-4A-99-ED	172.20.129.201	Mtto. Industrial	Superintendencia de Terminales y Depósitos

ANEXO 8: Teléfonos IP de la Red de Beaterio

TELEFONOS IP DE LA RED DE BEATERIO						
Extensión	**Origen**	**Dirección MAC**	**Función**	**Departamento**	**Usuario**	**Observaciones**
101	Beaterio	08:00:0F:07:1D:21	Serv.Técnico	Telecomunicaciones	Personal	
102	Beaterio	08:00:0F:05:0B:71		Jefatura de Mtto		Aun no instalado
103	Beaterio	08:00:0F:05:16:09	Secretaria	Productos Limpios	Marlene Valencia	
104	Beaterio	08:00:0F:01:B6:93	Jefatura	Jeft. de Terminal	Jaime Paez	
105	Beaterio	08:00:0F:07:26:23	Jefatura	Jeft. Mtto. Terminal	Francisco de la Torre	
106	Beaterio	08:00:0F:05:0A:B3	Secretaria	Superint. Terminales	Laura Mera	
107	Beaterio	08:00:0F:04:F4:24	Jefatura	Sucursal Quito	Enrique Paredes	
108	Beaterio	08:00:0F:07:24:6F	Secretaria	Sucursal Quito	Angela Suarez	
111	Beaterio	08:00:0F:0E:74:3B	Secretaria	Poliducto Q.A.R.	Azucena Espinoza	
114	Beaterio	08:00:0F:01:B7:88	Secretaria	Seguridad Industrial	Germania Flores	
115	Beaterio	08:00:0F:05:15:AA	Jefatura	Bodega	Jorge Jaramillo	
126	Beaterio	08:00:0F:05:15:B3	Operadores	Estación Reductora	Operadores	
130	Beaterio	08:00:0F:07:12:C0	Supervisor	Telecomunicaciones	Juan Lema	
202	Beaterio	08:00:0F:0E:73:56	Jefatura	Productos Limpios	Angel Cepeda	
389	Beaterio	08:00:0F:0E:73:39		Mtto Línea - Pol Q-A-R		
5106	Matriz	08:00:0F:0E:75:FB	Jefatura	Superint. Terminales	Franklin Cañadas	172.20.129.171
5113	Matriz	08:00:0F:0E:66:CC	Jefatura	Control de Calidad	Edgar Padilla	172.20.129.172
5114	Matriz	08:00:0F:0E:75:FC	Jefatura	Inspecciión técnica	Jorge Gonzalez	172.20.129.173
5121	Matriz	08:00:0F:0E:74:88	Serv.Técnico	Telecomunicaciones	Técnicos	172.20.129.174

ANEXO 9: Nuevo Direccionamiento IP para la Matriz con la Propuesta 1

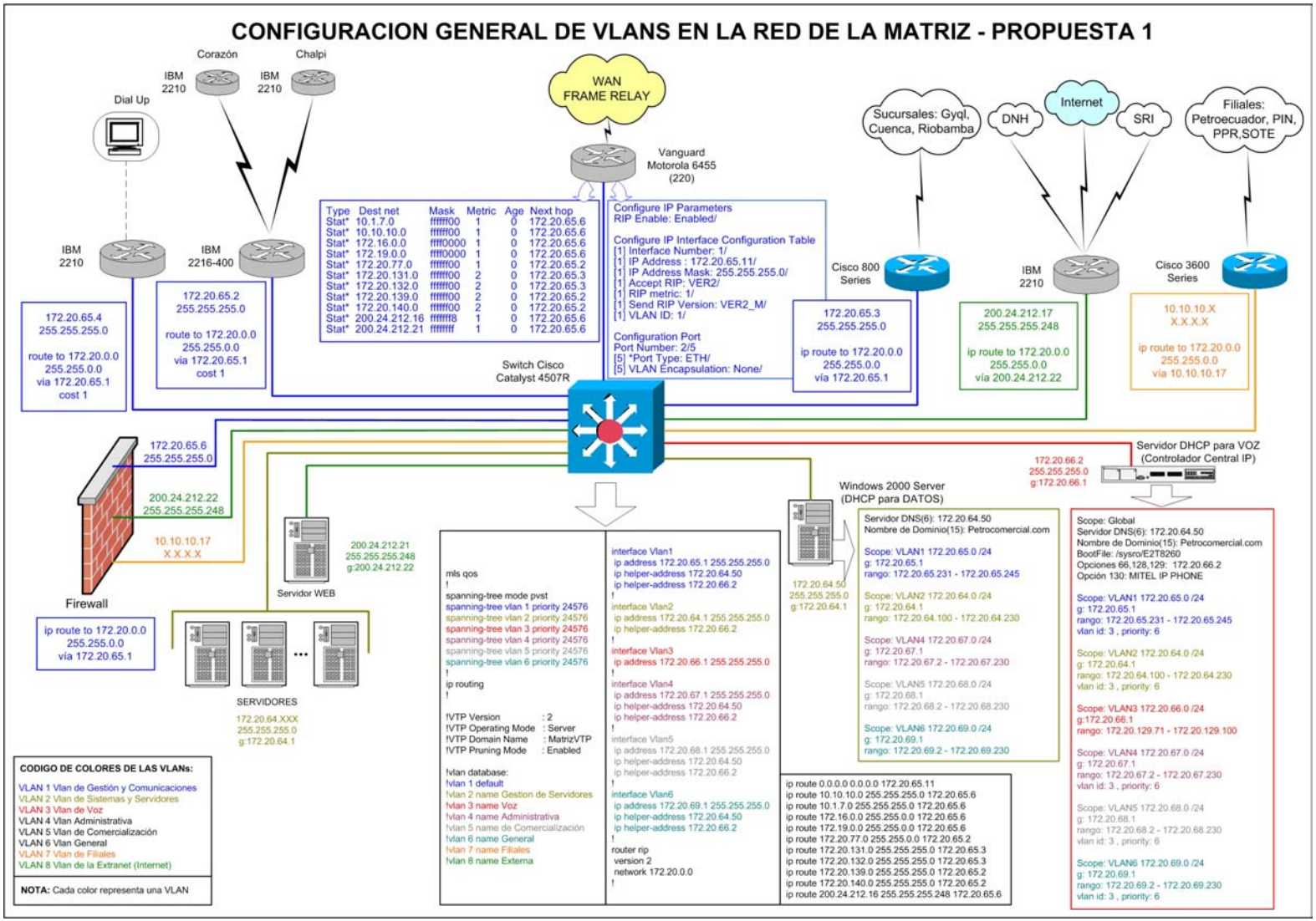
NUEVO DIRECCIONAMIENTO IP DE LA MATRIZ (172.20.64.0/21) PROPUESTA 1				
172.20.64.0/21	172.20.64.0/24	172.20.64.0		VLAN 2
		172.20.64.1	Gateway para la VLAN 2	
		…	Direcciones Libres	
		172.20.64.20 … 172.20.64.29	I-Series (AS/400's)	
		172.20.64.30 … 172.20.64.49	Direcciones para control del Firewall	
		172.20.64.50 … 172.20.64.69	Servidores	
		172.20.64.70 … 172.20.64.229	Scope del DHCP para las PC's de la VLAN de Gestion de Servidores	
		172.20.64.230 … 172.20.64.254	Impresoras para la VLAN DE GESTION DE SERVIDORES	
		172.20.64.255		
	172.20.65.0/24	172.20.65.0		VLAN 1
		172.20.65.1	Gateway para la VLAN 1 (SW 4507R)	
		172.20.65.2 … 172.20.65.19	Comunicaciones (Routers, RAS y Firewall)	
		172.20.65.20 … 172.20.65.100	Direcciones Libres	
		172.20.65.101 … 172.20.65.229	Switches Cisco	
		172.20.65.230 … 172.20.65.244	Scope del DHCP para las PC's de la VLAN de Gestión de Red	
		172.20.65.245 … 172.20.65.254	Impresoras para la VLAN DE GESTION DE RED	
		172.20.65.255		
	172.20.66.0/24	172.20.66.0		VLAN 3
		172.20.66.1	Gateway para la VLAN 3	
		172.20.66.2	Dirección Estática (Central Telf. IP)	
		172.20.66.3	Dirección estática del E2T (Central)	
		…		
		172.20.66.10 … 172.20.66.220	Direcciones asignadas al DHCP de la Cental IP Mitel para los teléfonos IP	
		… 172.20.66.255		
	172.20.67.0/24	172.20.67.0		VLAN 4
		172.20.67.1	Gateway para la VLAN 4	
		172.20.67.2 … 172.20.67.229	Scope del DHCP para las PC's de la VLAN Administrativa	
		172.20.67.230 … 172.20.67.254	Impresoras para la VLAN ADMINISTRATIVA	
		172.20.67.255		
	172.20.68.0/24	172.20.68.0		VLAN 5
		172.20.68.1	Gateway para la VLAN 5	
		172.20.68.2 … 172.20.68.229	Scope del DHCP para las PC's de la VLAN de Comercialización	
		172.20.68.230 … 172.20.68.254	Impresoras para la VLAN COMERCIALIZACION	
		172.20.68.255		
	172.20.69.0/24	172.20.69.0		VLAN 6
		172.20.69.1	Gateway para la VLAN 6	
		172.20.69.2 … 172.20.69.229	Scope del DHCP para las PC's de la VLAN General	
		172.20.69.230 … 172.20.69.254	Impresoras para la VLAN GENERAL	
		172.20.69.255		
		172.20.70.0 … 172.20.70.255		
		172.20.71.0 … 172.20.71.255		
	10.10.10.0/24	10.10.10.17	Filiales	VLAN 7
	200.24.212.16/29	200.24.212.17 … 200.24.212.22	Extranet (Internet)	VLAN 8

Detalle de Direcciones IP de la Matriz - Quito Red: 172.20.64.0/21			
PROPUESTA 2			
Rango	Detalle	Descripción	VLAN
64.1 - 64.126 Comunicaciones	.1	Router Vanguard Motorola	
	.2	Interfaz del Switch Multilayer al Router Vanguard	
	.5	Firewall IBM AIX (Interna)	
	.6	Interfaz del Switch Multilayer al Firewall IBM AIX	
	.9	Router CISCO 800 Series	
	.10	Interfaz del Switch Multilayer al Router Cisco 800 Series	
	.13	Router IBM 2216-400 (Corazón, Chalpi)	
	.14	Interfaz del Switch Multilayer al Router IBM 2216-400	
	.17	Router IBM 2210 Dial up	
	.18	Interfaz del Switch Multilayer al Router IBM 2210	
	.15 - .126	Libres	
64.129	.129	Switch Multilayer Cisco 4507R y Gateway para la VLAN 1	
64.130 - 64.169 Switches Cisco	.130	Switch Cisco Pco_66	VLAN1
	.131	Switch Cisco Pco_67	
	.132	Switch Cisco Pco_68	
	.133	Switch Cisco Pco_69	
	.134	Switch Cisco Pco_70	
	.135	Switch Cisco Pco_71	
	.136	Switch Cisco Pco_72	
	.137	Switch Cisco Pco_73	
	.138	Switch Cisco Pco_74	
	.139	Switch Cisco Pco_75	
	.140	Switch Cisco Pco_76	
	.141	Switch Cisco Pco_77	
	.142	Switch Cisco Pco_78	
65.170 - 65.199		Scope del DHCP para las PC's de la VLAN de Gestión de Red	
65.200 - 64.209 Impresoras			
.210 - .254		Libres	
65.1	.1	Gateway para la VLAN 2	
65.2 - 65.49 Direcciones para control del Firewall	.2 - .29	Libres	VLAN2
	.30	Libre	
	.31	Soporte de Aplicaciones (SSAFT)	
	.32	Libre	
	.33	Libre	
	.34	Libre	
	.35	Libre	
	.36	Libre	
	.37	Libre	
	.38	Libre	
	.39	Control de Gestión (VCGFE)	
	.40	Libre	
	.41	Seguros y Garantías (FSGMT)	
	.42	Seguros y Garantías (FSGMV)	
	.43	Libre	
	.44	Seguros y Garantías (FSGFG)	
	.45	Contratos de Contratos (GCCXE)	
	.46	Coordinación de Contratos (GCCWG)	
	.47	Coordinación de Contratos (GCCWG)	
	.48	Coordinación de Contratos (GCCWG)	
	.49	Libre	
65.50 - 65.69 Servidores Empresariales	.50	Pcored	
	.51	Pcored1	
	.52	Pcored2	
	.53	Pcored3	
	.54	Libre	
	.55	Libre	
	.56	Pcored6	
	.57	Pcored7	
	.58	Libre	
	.59	Libre	
	.60	Libre	
	.61	Libre	
	.62	Libre	
	.63	Libre	
	.64	Libre	
	.65	Libre	
	.66	Libre	
	.67	Libre	
	.68	Libre	
	.69	Libre	
65.70 - 65.229		Scope del DHCP para las PC's de la VLAN de Gestion de Servidores	
65.230 - 65.254 Impresoras	.236	Impresora Lexmark C720 (Soporte y Aplicaciones) 4to p	
	.238	Impresora IBM Infoprint 1145 (Sistemas) 5to p	
	.239	Impresora IBM Infoprint 1145 (Sistemas) 5to p	
	.240	Impresora Lexmark T522 (Sistemas y Telec.) 5to p	
	.241	Impresora Lexmark C720 (Sistemas y Telec.) 5to p	
	.250	Impresora Lexmark Optra 1650 (Mtto. Sistemas)Ex_pb	
66.1	.1	Gateway para la VLAN 3	
66.2	.2	Controlador de la Central IP Mitel	
66.3	.3	E2T de la Central IP Mitel	VLAN3
66.10 - 66.220		Direcciones del DHCP de la Central para la teléfonos IP	
67.1	.1	Gateway para la VLAN 4	
67.2 - 67.10 Servidores y AS400's	.2	Pco1	
	.3	Pco2	
	.4		
	.5		
	.6		
	.7	Pcored4	
	.8	Pcored5	
	.9		VLAN4
	.10		
67.11 - 67.229		Scope del DHCP para las PC's de la VLAN Administrativa	
67.230 - 67.254 Impresoras	.232	Impresora Lexmark Optra 1650 (Presupuesto)2do p	
	.238	Impresora Lexmark T522 (Servicios Admin.) 5to p	
	.239	Impresora Lexmark T522 (Servicios Admin.) 5to p	
	.244	Impresora Lexmark Optra 1650 (Contabilidad) 8vo p	
	.248	Impresora Lexmark Optra 1650 (Coor. Contratos) Ex_1er p	
68.1	.1	Gateway para la VLAN 5	
68.2 - 68.10 Servidores y AS400's	.2	Pco8	
	.3	Pco9	
	.4 - .10		
68.11 - 68.229		Scope del DHCP para las PC's de la VLAN de Comercialización	VLAN5
68.230 - 68.254 Impresoras	.232	Impresora Lexmark T522 (Abastecedora) 2do p	
	.233	Impresora Lexmark Optra 1650 (Abastecedora) 2do p	
	.234	Impresora Lexmark T522 (Comercializadora) 3er p	
	.243	Impresora HP (Subgerencia de Transporte) 7mo p	
69.1	.1	Gateway para la VLAN 6	
69.2 - 69.229		Scope del DHCP para las PC's de la VLAN General	VLAN6
69.230 - 69.254 Impresoras	.230	Impresora Lexmark T522 (Legal Gerencia Norte) 9no p	
70.1 - 71.254		Direcciones Libres	
10.10.10.17	.17	Firewall IBM AIX (Filiales)	VLAN7
200.24.212.17	.17	Router IBM 2210 (INTERNET, SRI, DNH)	
200.24.212.18	.18	NAT de PCO8	
200.24.212.19	.19	Libre	VLAN8
200.24.212.20	.20	Libre	
200.24.212.21	.21	Pcoweb	
200.24.212.22	.22	Firewall IBM AIX (Externa)	

DIRECCIONES IP DE IMPRESORAS DE RED DE LA MATRIZ - PROPUESTA 1			
64.230 - 64.254 Impresoras	.230	Impresora 1er piso	VLAN2
	.231	Impresora 1er piso	
	.232	Impresora 2do piso	
	.233	Impresora 2do piso	
	.234	Impresora 3er piso	
	.235	Impresora 3er piso	
	.236	Impresora Lexmark C720 (Soporte y Aplicaciones) 4to p	
	.237	Impresora 4to piso	
	.238	Impresora IBM Infoprint 1145 (Sistemas) 5to p	
	.239	Impresora IBM Infoprint 1145 (Sistemas) 5to p	
	.240	Impresora Lexmark T522 (Sistemas y Telec.) 5to p	
	.241	Impresora Lexmark C720 (Sistemas y Telec.) 5to p	
	.242	Impresora 6to piso	
	.243	Impresora 6to piso	
	.244	Impresora 7mo piso	
	.245	Impresora 7mo piso	
	.246	Impresora 8vo piso	
	.247	Impresora 8vo piso	
	.248	Impresora 9no piso	
	.249	Impresora 9no piso	
	.250	Impresora Lexmark Optra 1650 (Mtto. Sistemas)Ex_pb	
	.251	Impresora Ex - salesianos	
66.230 - 66.254 Impresoras	.230	Impresora 1er piso	VLAN4
	.231	Impresora 1er piso	
	.232	Impresora Lexmark Optra 1650 (Presupuesto)2do p	
	.233	Impresora 2do piso	
	.234	Impresora 3er piso	
	.235	Impresora 3er piso	
	.236	Impresora 4to piso	
	.237	Impresora 4to piso	
	.238	Impresora Lexmark T522 (Servicios Admin.) 5to p	
	.239	Impresora Lexmark T522 (Servicios Admin.) 5to p	
	.240	Impresora 6to piso	
	.241	Impresora 6to piso	
	.242	Impresora 7mo piso	
	.243	Impresora 7mo piso	
	.244	Impresora Lexmark Optra 1650 (Contabilidad) 8vo p	
	.245	Impresora 8vo piso	
	.246	Impresora 9no piso	
	.247	Impresora 9no piso	
	.248	Impresora Lexmark Optra 1650 (Coor. Contratos) Ex_1er p	
	.249	Impresora Ex - salesianos	
67.230 - 67.254 Impresoras	.230	Impresora 1er piso	VLAN5
	.231	Impresora 1er piso	
	.232	Impresora Lexmark T522 (Abastecedora) 2do p	
	.233	Impresora Lexmark Optra 1650 (Abastecedora) 2do p	
	.234	Impresora Lexmark T522 (Comercializadora) 3er p	
	.235	Impresora 3er piso	
	.236	Impresora 4to piso	
	.237	Impresora 4to piso	
	.238	Impresora 5to piso	
	.239	Impresora 5to piso	
	.240	Impresora 6to piso	
	.241	Impresora 6to piso	
	.242	Impresora 7mo piso	
	.243	Impresora HP (Subgerencia de Transporte) 7mo p	
	.244	Impresora 8vo piso	
	.245	Impresora 8vo piso	
	.246	Impresora 9no piso	
	.247	Impresora 9no piso	
	.248	Impresora Ex - salesianos	
	.249	Impresora Ex - salesianos	
68.230 - 68.254 Impresoras	.230	Impresora Lexmark T522 (Legal Gerencia Norte) 9no p	VLAN6
	.231	Impresora 1er piso	
	.232	Impresora 2do piso	
	.233	Impresora 2do piso	
	.234	Impresora 3er piso	
	.235	Impresora 3er piso	
	.236	Impresora 4to piso	
	.237	Impresora 4to piso	
	.238	Impresora 5to piso	
	.239	Impresora 5to piso	
	.240	Impresora 6to piso	
	.241	Impresora 6to piso	
	.242	Impresora 7mo piso	
	.243	Impresora 7mo piso	
	.244	Impresora 8vo piso	
	.245	Impresora 8vo piso	
	.246	Impresora 9no piso	
	.247	Impresora 9no piso	
	.248	Impresora Ex - salesianos	
	.249	Impresora Ex - salesianos	

RESUMEN DEL RANGO DE DIRECCIONES IP PARA CADA VLAN DE LA MATRIZ - PROPUESTA 1						
VLAN #	**Nombre**	**Rango Util de direcciones**	**Máscara**	**/#**	**Nro. De Clientes**	**Común acceso a:**
VLAN 2	Vlan de Gestión de Red	172.20.64.1 - 172.20.64.254	255.255.255.0	/24	24	
VLAN 1	Vlan de Gestion de Servidores	172.20.65.1 - 172.20.65.254	255.255.255.0	/24	51	
VLAN 3	Vlan de Voz	172.20.66.1 - 172.20.66.254	255.255.255.0	/24	139	
VLAN 4	Vlan Administrativa	172.20.67.1 - 172.20.67.254	255.255.255.0	/24	121	PCO1,PCO2, PCORED4, PCORED5
VLAN 5	Vlan de Comercialización	172.20.68.1 - 172.20.68.254	255.255.255.0	/24	60	PCO8, PCO9
VLAN 6	Vlan General	172.20.69.1 - 172.20.69.254	255.255.255.0	/24	64	PCORED, PCORED1, PCORED7
VLAN 7	Vlan de Filiales	10.10.10.17			1	
VLAN 8	Vlan de la Extranet (Internet)	200.24.212.17 - 200.24.212.22	255.255.255.248	/29	6	

ANEXO 10: Configuración de VLANs en la Red de la Matriz con la Propuesta 1



ANEXO 11: Nuevo Direccionamiento IP para Beaterio con la Propuesta 1

NUEVO DIRECCIONAMIENTO IP DEL BEATERIO (172.20.129.0/24) PROPUESTA 1				
172.20.129.0/24	172.20.129.0/27	172.20.129.0		VLAN 1
		172.20.129.1 … 172.20.129.10	Switches y **Gateway para VLAN 1 (172.20.129.1)**	
		172.20.129.11 … 172.20.129.20	Routers	
		172.20.129.21 … 172.20.129.30	Direcciones para las PC's de la **VLAN de GESTION** usando el DHCP de la Central Mitel	
		172.20.129.31		
	172.20.129.32/27	172.20.129.32		VLAN 2
		172.20.129.33	**Gateway para VLAN 2**	
		172.20.129.34 … 172.20.129.62	Proyecto de Automatización y Control (**VLAN de AUTOMATIZACION**)	
		172.20.129.63		
	172.20.129.64/26	172.20.129.64		VLAN 3
		172.20.129.65	**Gateway para VLAN 3**	
		…		
		172.20.129.68	Dir.estática de una PC para upgrade de software de la Central	
		172.20.129.69	Dirección estática del E2T (Central)	
		172.20.129.70	Dirección estática de la Central Telf. IP MITEL	
		172.20.129.71 … 172.20.129.100	Direcciones del DHCP de la Central para los teléfonos IP (**VLAN de VOZ**)	
		…		
		172.20.129.127		
	172.20.129.128/25	172.20.129.128		VLAN 4
		172.20.129.129	**Gateway para VLAN 4**	
		172.20.129.130 … 172.20.129.254	Direcciones para las PC's de la **VLAN de DATOS** usando el DHCP de la Central Mitel	
		172.20.129.255		

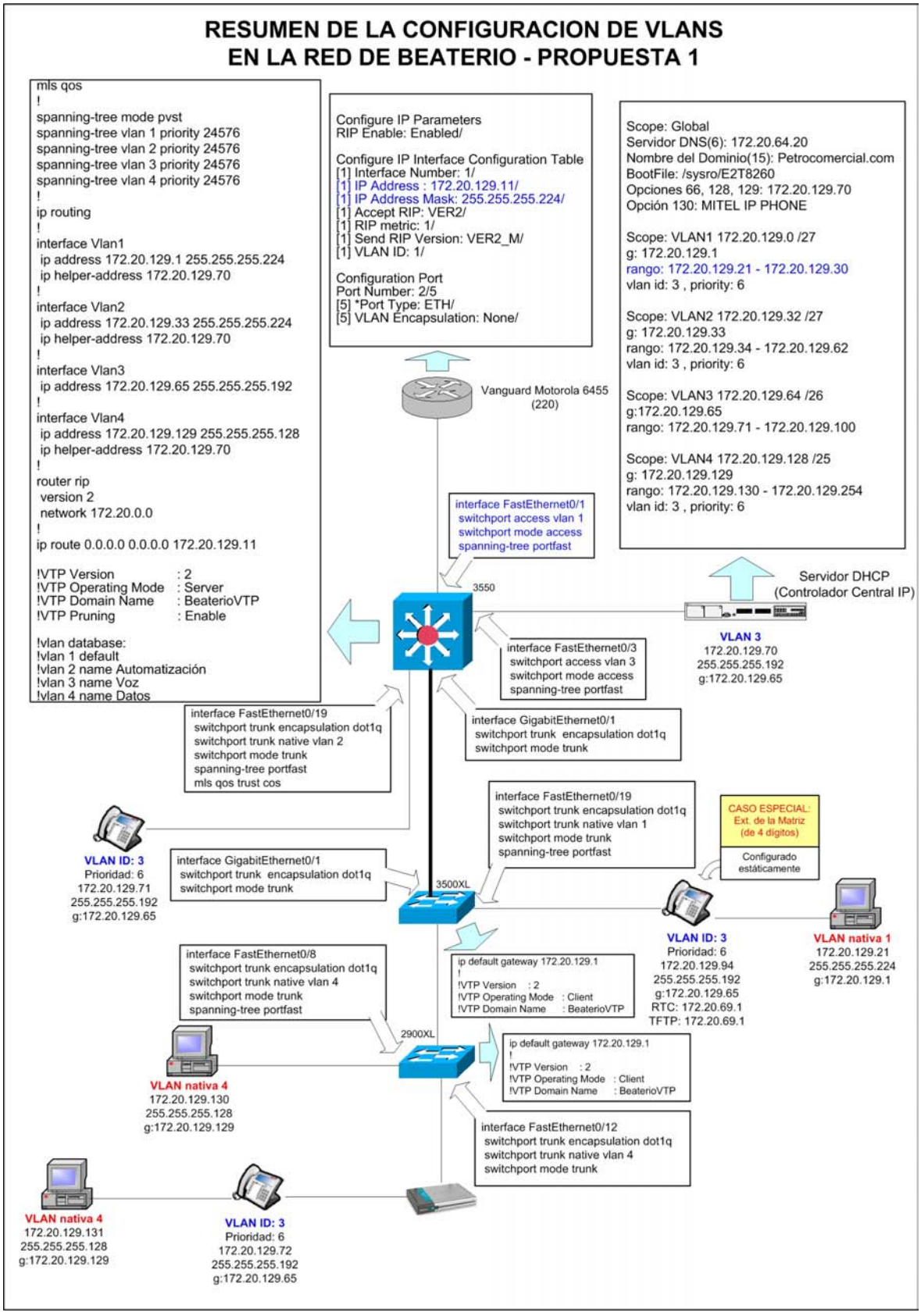
Detalle de Nuevas Direcciones IP de Beaterio - Quito
Red: 172.20.129.0/24 - PROPUESTA 1

Rango	Detalle	Descripción	VLAN#
129.1 - 129.10 Switches	172.20.129.1	Switch Cisco Catalyst 3550 Series y **Gateway para la VLAN 1**	VLAN1
	172.20.129.2	Switch Cisco Catalyst 3500 XL Series	
	172.20.129.3	Switch Cisco Catalyst 2900 XL Series	
	.4 - .10	Libres	
129.11 - 129.20 Routers	172.20.129.11	Router Motorola Vanguard 6455 (220)	
	172.20.129.12	Router Motorola Vanguard 6455 (221)	
	.13 - .20	Libres	
129.21 - 129.30		Direcciones para las PC's de la **VLAN de GESTION** usando el DHCP de la Central Mitel	
.129.33	172.20.129.33	**Gateway para VLAN 2**	VLAN2
129.34 - .129.62		Proyecto de Automatización y Control (**VLAN de AUTOMATIZACION**)	
129.65	172.20.129.65	**Gateway para VLAN 3**	VLAN3
.66 - .67		Libres	
129.68	172.20.129.68	PC para upgrade de software de la Central	
129.69	172.20.129.69	E2T de la Central IP Mitel	
129.70	172.20.129.70	Controlador de la Central IP Mitel	
129.71 - 129.100		Direcciones del DHCP de la Central para los teléfonos IP (**VLAN De VOZ**)	
129.100 - 129.126		Libres	
129.129	172.20.129.129	**Gateway para VLAN 4**	VLAN4
.129.130 - .129.254		Direcciones para las PC's de la **VLAN de DATOS** usando el DHCP de la Central Mitel	

RESUMEN DEL RANGO DE DIRECCIONES IP PARA CADA VLAN DE BEATERIO - PROPUESTA 1

VLAN #	Nombre	Rango Util de direcciones	Máscara	/#	Nro. De Clientes
VLAN 1	VLAN de Gestion	172.20.129.1 - 172.20.129.30	255.255.255.224	/27	6
VLAN 2	VLAN de Automatización	172.20.129.33 - 172.20.129.62	255.255.255.224	/27	15
VLAN 3	VLAN de Voz	172.20.129.65 - 172.20.129.126	255.255.255.192	/26	20
VLAN 4	VLAN de Datos	172.20.129.129 - 172.20.129.254	255.255.255.128	/25	36

ANEXO 12: Configuración de VLANs en la Red de Beaterio – Propuesta 1



ANEXO 13: Configuración de Rutas estáticas de los Routers de la Matriz

Router IBM2216-400 (Corazón, Chalpi, Quijos) 172.20.64.2

route to 172.20.97.0 ,255.255.255.0 via 172.20.32.10 cost 1
route to 172.20.0.0 ,255.255.0.0 via 172.20.64.11 cost 1
route to 172.20.139.0 ,255.255.255.0 via 172.20.32.17 cost 1
route to 172.20.140.0 ,255.255.255.0 via 172.20.32.13 cost 1
route to 172.20.77.0 ,255.255.255.0 via 172.20.32.5 cost 1

Router IBM2210 (Acceso Dial-Up) 172.20.64.4

route to 172.20.0.0 ,255.255.255.0 via 172.20.64.11 cost 1

Router IBM2210 (Internet, DNH, SRI) 200.24.212.17

route to 0.0.0.0 ,0.0.0.0 via 200.24.212.9 cost 1
route to 172.20.71.5 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.20.71.6 ,255.255.255.255 via 200.24.212.2 cost 1
route to 10.1.7.0 ,255.255.255.0 via 168.20.40.2 cost 1
route to 200.24.212.19 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.20.64.31 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.20.134.26 ,255.255.255.255 via 200.24.212.2 cost 1
route to 200.24.212.18 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.16.1.0 ,255.255.255.0 via 168.20.40.6 cost 1
route to 200.24.212.20 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.16.2.0 ,255.255.255.0 via 168.20.40.6 cost 1
route to 172.20.71.7 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.20.71.21 ,255.255.255.255 via 200.24.212.2 cost 1
route to 192.190.10.126 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.19.48.80 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.17.24.44 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.17.24.74 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.17.24.103 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.19.208.88 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.17.20.22 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.17.16.23 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.17.28.22 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.17.24.22 ,255.255.255.255 via 200.24.212.2 cost 1
route to 172.17.16.22 ,255.255.255.255 via 200.24.212.2 cost 1

Router IBM2210 (Chalpi) 172.20.139.10

route to 0.0.0.0 ,0.0.0.0 via 172.20.32.18 cost 1

Router Vanguard 6455 (Acceso a WAN Frame RelayI) 172.20.64.11

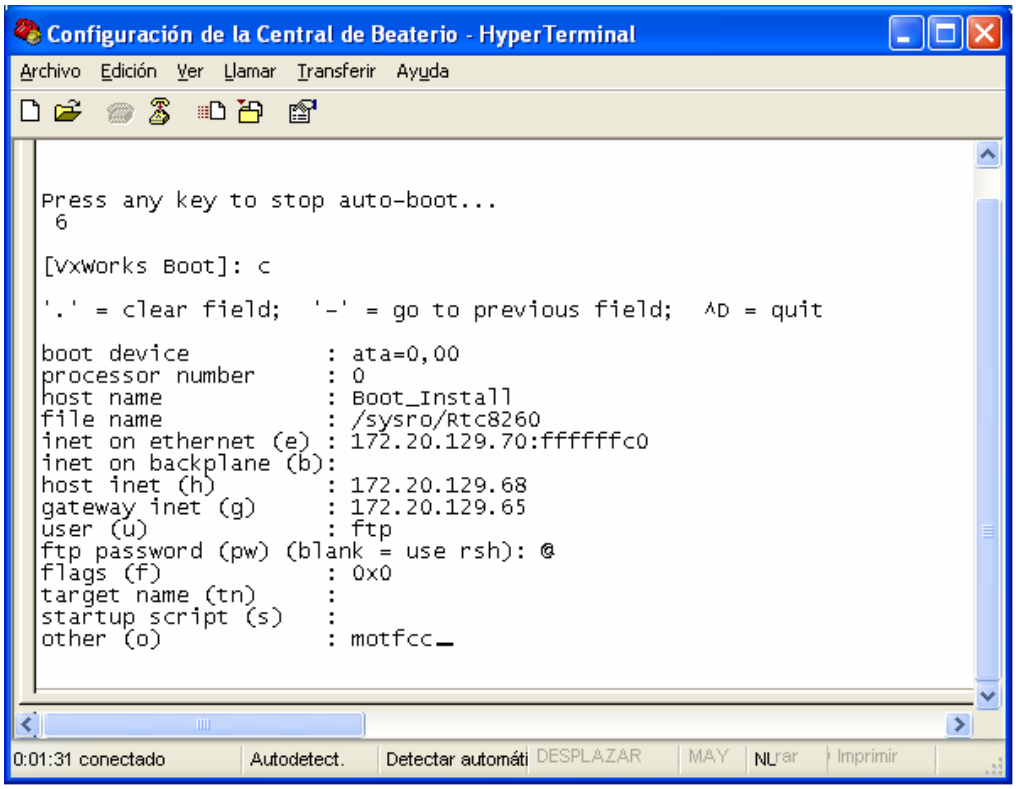
Type	Dest net	Mask	Metric	Age	Next hop
Stat*	0.0.0.0		0 10	0	172.20.64.10
Sbnt	10.0.0.0	ff000000	1	0	None
Stat*	10.1.7.0	ffffff00	1	0	172.20.64.6
Stat*	10.10.10.0	ffffff00	1	0	172.20.64.6
Stat*	172.16.0.0	ffff0000	1	0	172.20.64.6
Sbnt	172.17.0.0	ffff0000	1	0	None
RIP	172.17.16.0	ffffff00	2	20	172.20.36.26
Stat*	172.17.28.0	ffffff00	2	0	172.20.36.26
Stat*	172.19.0.0	ffff0000	1	0	172.20.64.6
Sbnt	172.20.0.0	ffff0000	1	0	172.20.64.10
RIP	172.20.32.92	fffffffc	2	20	172.20.36.10
Dir	172.20.36.0	fffffffc	1	0	SL/5
Dir	172.20.36.4	fffffffc	1	0	SL/6
Dir	172.20.36.8	fffffffc	1	0	SL/7
Dir	172.20.36.12	fffffffc	1	0	SL/8
Dir	172.20.36.16	fffffffc	1	0	SL/9
Dir	172.20.36.20	fffffffc	1	0	SL/10
Dir	172.20.36.24	fffffffc	1	0	SL/11
RIP	172.20.36.28	fffffffc	2	30	172.20.36.14
RIP	172.20.36.36	fffffffc	3	30	172.20.36.26
RIP	172.20.36.40	fffffffc	2	30	172.20.36.26
RIP	172.20.36.44	fffffffc	2	30	172.20.36.26
RIP	172.20.36.48	fffffffc	3	30	172.20.36.26
RIP	172.20.36.52	fffffffc	2	30	172.20.36.26
RIP	172.20.36.56	fffffffc	3	30	172.20.36.26
RIP	172.20.36.60	fffffffc	3	30	172.20.36.26
RIP	172.20.36.64	fffffffc	3	30	172.20.36.26
Dir	172.20.36.68	fffffffc	1	0	SL/20
Dir	172.20.36.128	fffffffc	1	0	SL/12
Dir	172.20.36.132	fffffffc	1	0	SL/13
Dir	172.20.36.136	fffffffc	1	0	SL/14
Dir	172.20.36.152	fffffffc	1	0	SL/15
Dir	172.20.36.156	fffffffc	1	0	SL/16
Dir	172.20.36.160	fffffffc	1	0	SL/17
Dir	172.20.36.164	fffffffc	1	0	SL/18
Dir	172.20.36.168	fffffffc	1	0	SL/19
RIP	172.20.39.8	fffffffc	2	30	172.20.36.26
RIP	172.20.39.24	fffffffc	2	30	172.20.36.26
RIP	172.20.39.28	fffffffc	2	30	172.20.36.26
RIP	172.20.40.4	fffffffc	2	10	172.20.36.138
RIP	172.20.40.96	ffffffe0	2	0	172.20.36.2
Dir	172.20.64.0	fffff800	1	0	ETH/2
Dir	172.20.64.11	ffffffff	1	0	INT/37
Stat*	172.20.75.0	ffffff00	1	0	172.20.36.22
RIP	172.20.76.0	ffffff00	2	20	172.20.36.170
Stat*	172.20.77.0	ffffff00	1	0	172.20.64.2
Stat*	172.20.97.0	ffffff00	1	0	172.20.36.26
RIP	172.20.129.0	ffffff00	2	0	172.20.36.14
RIP	172.20.129.32	ffffffe0	3	0	172.20.36.14
RIP	172.20.129.64	ffffffc0	3	0	172.20.36.14
RIP	172.20.129.128	ffffff80	3	0	172.20.36.14
Stat*	172.20.130.0	ffffff00	3	0	172.20.36.6
Stat*	172.20.131.0	ffffff00	1	0	172.20.64.3
Stat*	172.20.132.0	ffffff00	1	0	172.20.64.3
Stat*	172.20.133.0	ffffff00	1	0	172.20.36.26
RIP	172.20.134.0	ffffff00	2	0	172.20.36.18
RIP	172.20.136.0	ffffff00	2	0	172.20.36.158
RIP	172.20.137.0	ffffff00	2	30	172.20.36.162
RIP	172.20.138.0	ffffff00	2	20	172.20.36.166
Stat*	172.20.139.0	ffffff00	1	0	172.20.64.2
Stat*	172.20.140.0	ffffff00	1	0	172.20.64.2
RIP	172.20.161.0	ffffff00	2	10	172.20.36.10
RIP	172.20.162.0	ffffff00	2	10	172.20.36.10
Stat*	172.20.163.0	ffffff00	1	0	172.20.36.134
RIP	172.20.164.0	ffffff00	2	20	172.20.36.138
Stat*	172.20.165.0	ffffff00	2	0	172.20.36.26
RIP	172.20.165.0	ffffffc0	3	10	172.20.36.26
RIP	172.20.165.64	ffffffc0	2	10	172.20.36.26
Stat*	172.20.167.0	ffffffc0	3	0	172.20.36.26
Stat*	172.20.167.64	ffffffc0	3	0	172.20.36.26
Stat*	172.20.167.128	ffffffc0	3	0	172.20.36.26
Stat*	172.20.169.0	ffffff00	3	0	172.20.36.26
Stat*	172.20.170.0	ffffffc0	3	0	172.20.36.26
Stat*	172.20.170.64	ffffffc0	3	0	172.20.36.26
Stat*	172.20.170.128	ffffffc0	3	0	172.20.36.26
Stat*	172.20.170.192	ffffffc0	3	0	172.20.36.26
Stat*	172.20.171.0	ffffffc0	1	0	172.20.36.70
Sbnt	200.24.212.0	ffffff00	1	0	None
Stat*	200.24.212.16	fffffff8	1	0	172.20.64.6
Stat*	200.24.212.21	ffffffff	1	0	172.20.64.6

Default gateway in use.

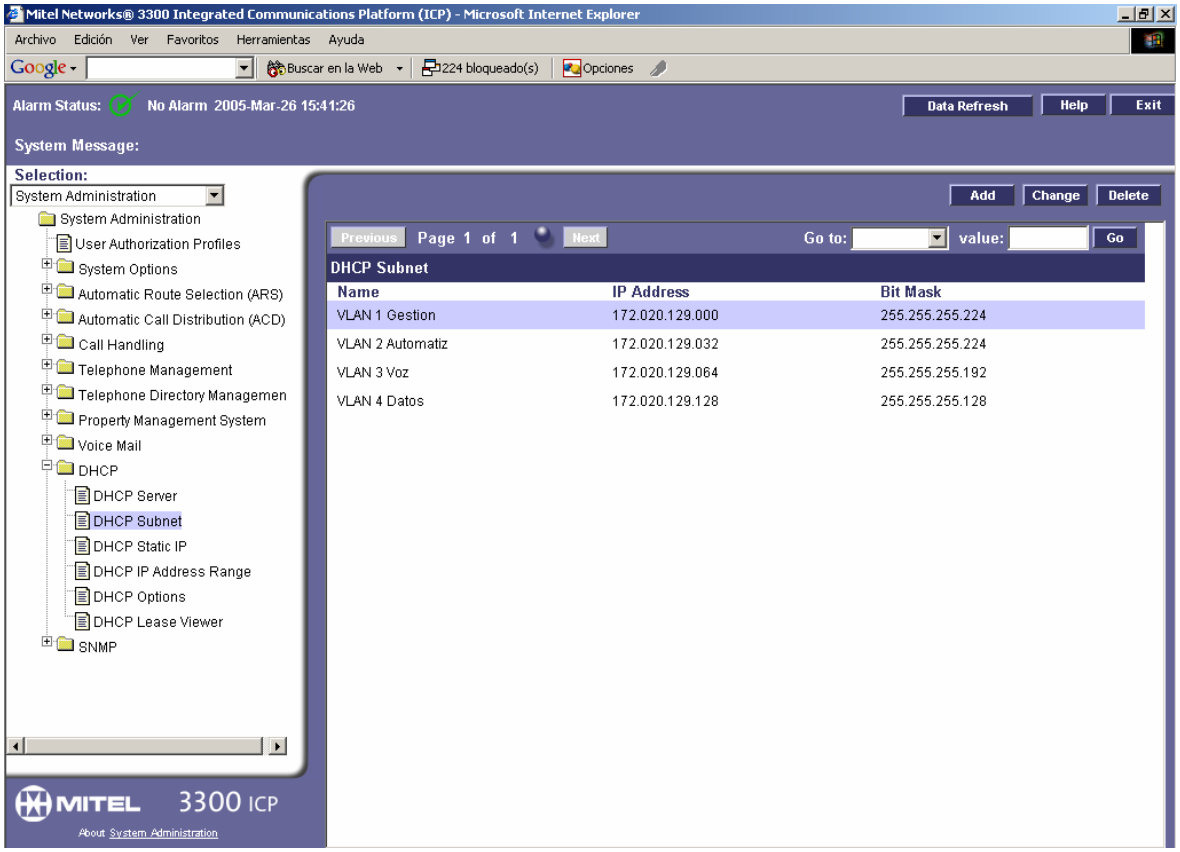
Type	Cost	Age	Next hop
Stat	10	0	172.20.64.10

ANEXO 14: Configuración del DHCP de la Central IP Mitel de Beaterio

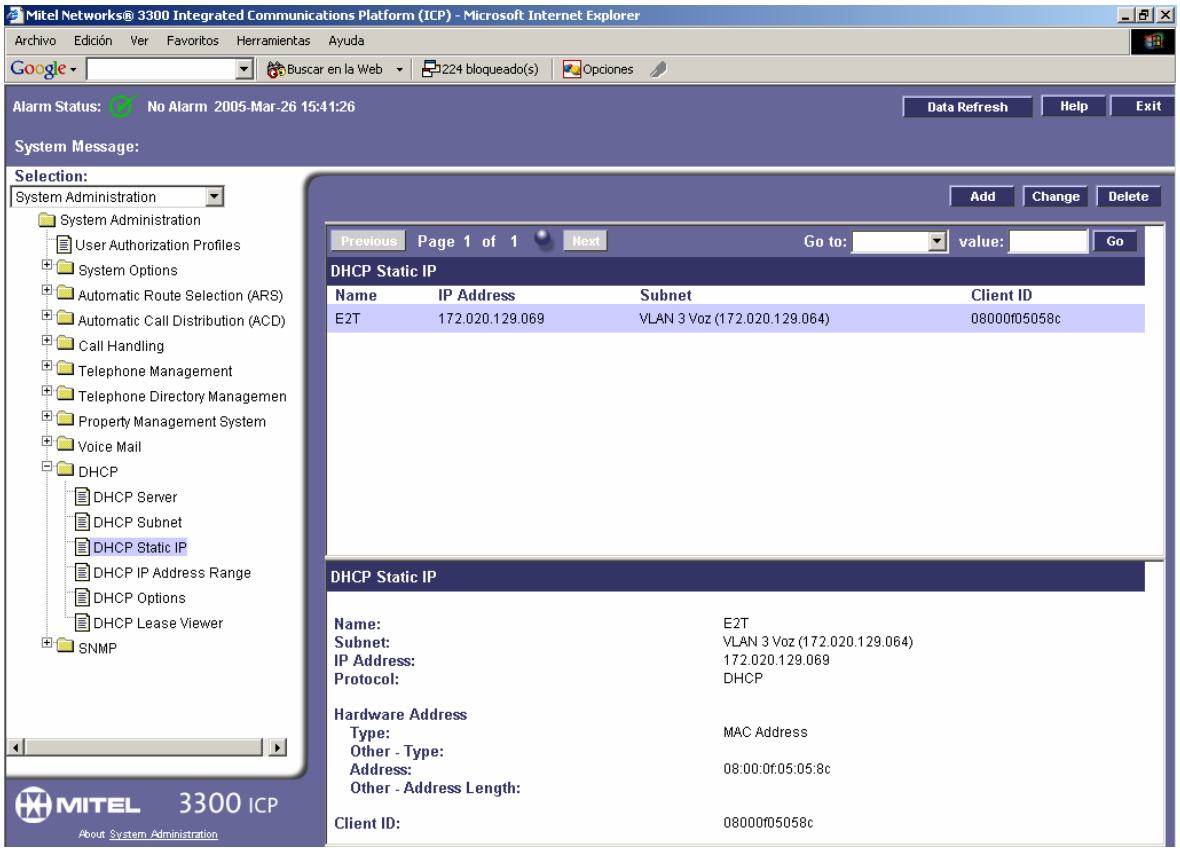
Configuración de la dirección IP del Controlador RTC de Beaterio:



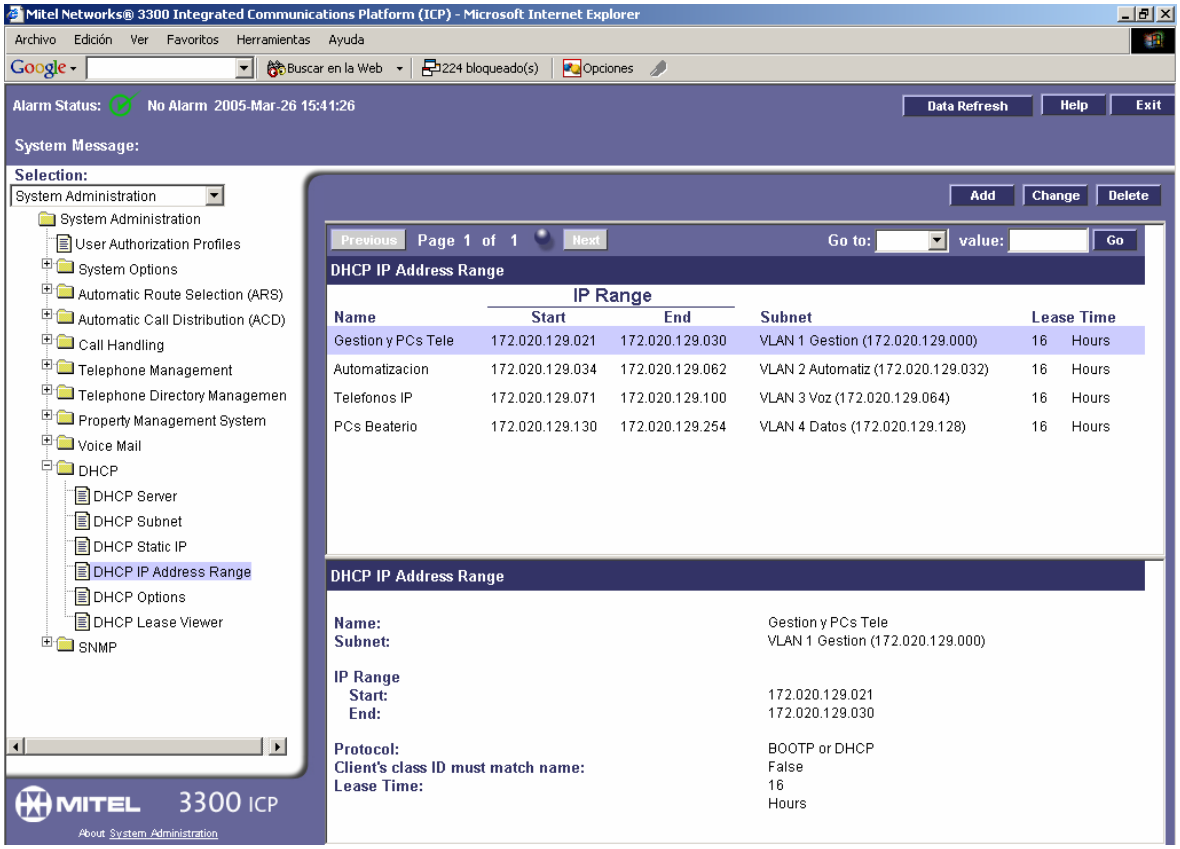
Configuración del **DHCP Subnet**:



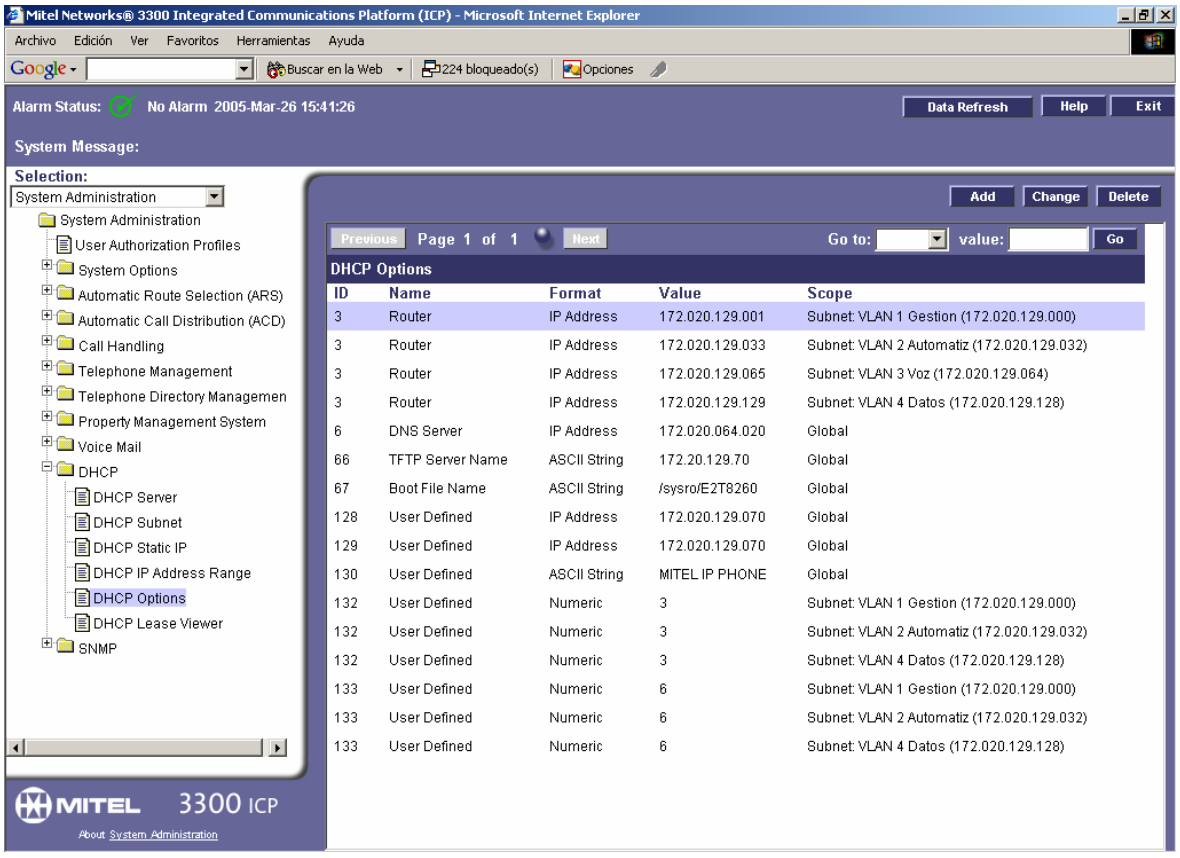
Configuración del **DHCP Static IP**:



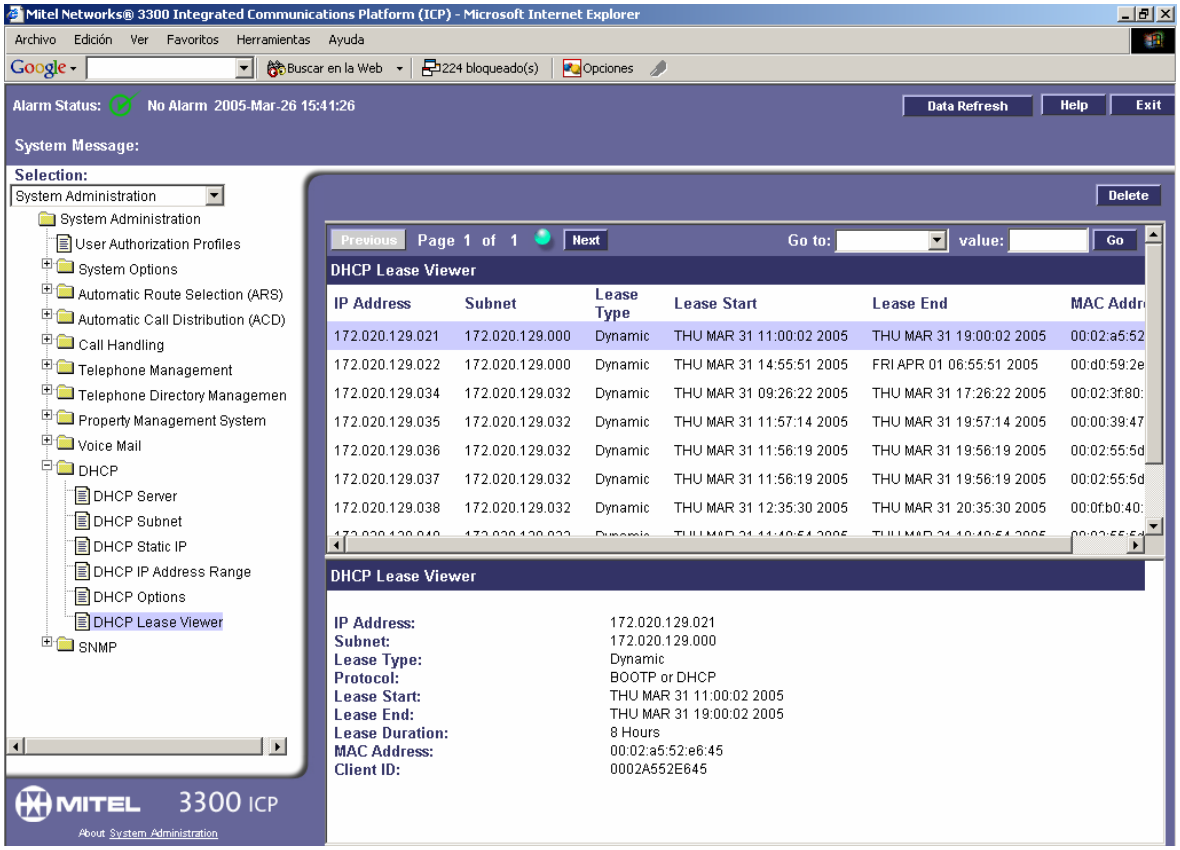
Configuración de **DHCP IP Address Range:**



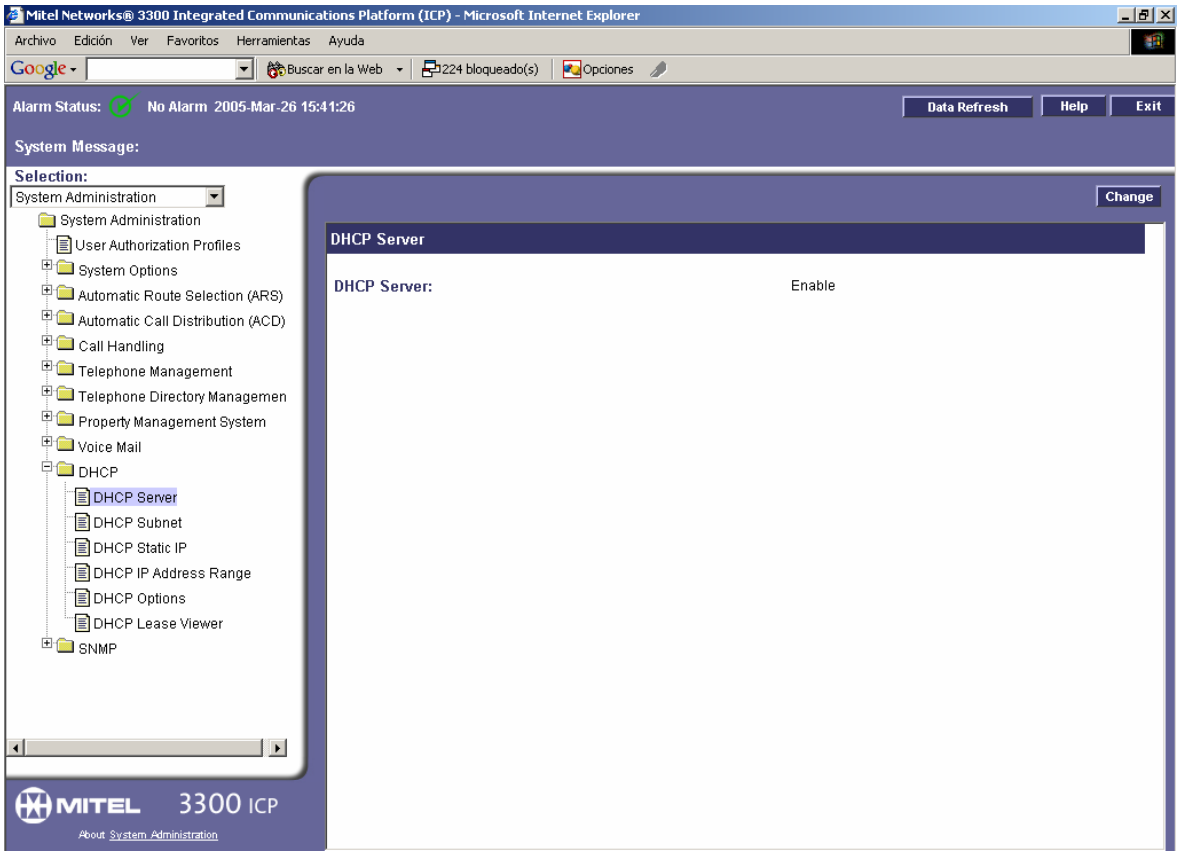
Configuración de **DHCP Options**:



Visualización de **DHCP Lease Viewer:**



Habilitación del **DHCP Server** del Controlador:



ANEXO 15: Hosts de la Red de Beaterio con la respectiva Asignación de VLANs

HOSTS DE LA RED DE BEATERIO CON LA RESPECTIVA ASIGNACIÓN DE VLANS											
SW #	Switch	Puerto	Nombre de Maquina	Usuario	MAC	Departamento	Unidad	Ext. IP	MAC del Telef.	VLAN Nativa	VLAN acceso
SW1	SW CISCO 3550	1		172.20.129.11	00-08-D5-00-05-41	Router 6455 (220)					1
SW1	SW CISCO 3550	2		172.20.129.229	00-02-AE-00-15-37	Net Buffer de la Central IP MITEL					4
SW1	SW CISCO 3550	3		172.20.129.70	08-00-0F-05-05-8C	Central Telefónica MITEL		Central	08-00-0F-05-18-A7		3
SW1	SW CISCO 3550	4									4
SW1	SW CISCO 3550	5									4
SW1	SW CISCO 3550	6									4
SW1	SW CISCO 3550	7	SRTJL	Técnicos (Compaq)	00-02-A5-52-E6-45	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	101	08-00-0F-07-1D-21	1	
SW1	SW CISCO 3550	8	GSTIA	Técnicos (IBM)	00-09-6B-E2-0A-DB	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	5121	08-00-0F-0E-74-88	1	
SW1	SW CISCO 3550	9									4
SW1	SW CISCO 3550	10									4
SW1	SW CISCO 3550	11									4
SW1	SW CISCO 3550	12									4
SW1	SW CISCO 3550	13	STDFC	Franklin Cañadas	00-02-55-5D-B4-E1	Superint. de Terminales	Superintendencia de Terminales y Depósitos	5106	08-00-0F-0E-75-FB	4	
SW1	SW CISCO 3550	14	PJC01	Francisco de la Torre	00-00-39-D4-D3-AD	Jef. Mtto.Terminal (Portatil)	Superintendencia de Terminales y Depósitos	105	08-00-0F-07-26-23	4	
SW1	SW CISCO 3550	15	YMTGJM	Secretaria de Superint	00-09-6B-C4-23-83	Superint. de Terminales	Superintendencia de Terminales y Depósitos			4	
SW1	SW CISCO 3550	16									4
SW1	SW CISCO 3550	17									4
SW1	SW CISCO 3550	18	SRTCS1	Juan Lema (portatil)	00-D0-59-2E-52-24	Redes y Telecomunicaciones	Sistemas y Telecomunicaciones	130	08-00-0F-07-12-C0	1	
SW1	SW CISCO 3550	19									4
SW1	SW CISCO 3550	20									4
SW1	SW CISCO 3550	21									4
SW1	SW CISCO 3550	22									4
SW1	SW CISCO 3550	23	A Switch de Mtto. Eléctrico			Jef. Mtto. Terminal	Superintendencia de Terminales y Depósitos				2
SW1	SW CISCO 3550	24	QJMCL	Jet - Fuel	00-02-55-5D-B6-41	Jet - Fuel	Superintendencia de Terminales y Depósitos				2
SW2	SW CISCO 3500XL	1	MOPRO2	Mopro	00-10-5A-A5-F1-26	Mopro	MOPRO			4	
SW2	SW CISCO 3500XL	2									4
SW2	SW CISCO 3500XL	3	MOPRO1	Mopro	00-02-A5-65-E4-04	Mopro	MOPRO			4	
SW2	SW CISCO 3500XL	4									4
SW2	SW CISCO 3500XL	5									4
SW2	SW CISCO 3500XL	6									4
SW2	SW CISCO 3500XL	7	YTBAC	Angel Cepeda	00-08-02-21-B2-43	Produtos Limpios	Superintendencia de Terminales y Depósitos			4	
SW2	SW CISCO 3500XL	8									4
SW2	SW CISCO 3500XL	9									4
SW2	SW CISCO 3500XL	10									4
SW2	SW CISCO 3500XL	11									4
SW2	SW CISCO 3500XL	12									4
SW2	SW CISCO 3500XL	13		Jaime Paez		Jefatura de Terminal	Superintendencia de Terminales y Depósitos	104	08-00-0F-01-B6-93	4	
SW2	SW CISCO 3500XL	14	A Switch de Sucursal							4	
SW2	SW CISCO 3500XL	15									4
SW2	SW CISCO 3500XL	16	A Switch de Bodega							4	
SW2	SW CISCO 3500XL	17		Angel Cepeda		Produtos Limpios	Superintendencia de Terminales y Depósitos	202	08-00-0F-0E-73-56	4	
SW2	SW CISCO 3500XL	18									4
SW2	SW CISCO 3500XL	19	TITJG	Jorge Gonzalez	00-02-A5-27-78-3B	Inspección Técnica	Inspección Técnica	5114	08-00-0F-0E-75-FC	4	
SW2	SW CISCO 3500XL	20	YTBNV	Marlene Valencia	00-60-94-EA-14-91	Produtos Limpios	Superintendencia de Terminales y Depósitos	103	08-00-0F-05-16-09	4	
SW2	SW CISCO 3500XL	21	TYEEF	Raúl Baldeón	00-10-5A-86-0C-95	Jef. Mtto. Terminal	Superintendencia de Terminales y Depósitos			4	
SW2	SW CISCO 3500XL	21		Raúl Baldeón (portatil)	00-50-BA-79-DF-3F	Jef. Mtto. Terminal	Superintendencia de Terminales y Depósitos			4	
SW2	SW CISCO 3500XL	22	A Switch de Control de Calidad							4	
SW2	SW CISCO 3500XL	23	QJM11	Paola Badillo	00-10-5A-28-EE-A5	Jef. Mtto. Terminal	Superintendencia de Terminales y Depósitos			4	
SW2	SW CISCO 3500XL	24		Secretaria de Superint				106	08-00-0F-05-0A-B3	4	
SW3	SW CISCO 2900XL	1	BSQLM		00-09-6B-BA-32-F2	Sucursal Quito (Comercializadora)	Abastecedora			4	
SW3	SW CISCO 2900XL	2	BSQAS	Angela Suarez	00-04-AC-53-75-A8	Sucursal Quito (Comercializadora)	Abastecedora	108	08-00-0F-07-24-6F	4	
SW3	SW CISCO 2900XL	3	DMBGM	Sra. Gladys - Dispensario	00-02-A5-36-EC-69	Dispensario Médico (Bienestar Laboral)	Administrativa			4	
SW3	SW CISCO 2900XL	4	DMOBJM	Dispensario	00-02-A5-36-A7-5C	Dispensario Médico (Bienestar Laboral)	Administrativa			4	
SW3	SW CISCO 2900XL	5	BSQMB		00-02-55-3B-8D-D4	Sucursal Quito (Comercializadora)	Abastecedora			4	
SW3	SW CISCO 2900XL	6									4
SW3	SW CISCO 2900XL	7									4
SW3	SW CISCO 2900XL	8	BSQEP	Jefatura	00-09-6B-BA-33-1A	Sucursal Quito (Comercializadora)	Abastecedora	107	08-00-0F-04-F4-24	4	
SW3	SW CISCO 2900XL	9	A Switch Dlink de Sucursal							4	
SW3	SW CISCO 2900XL	10									4
SW3	SW CISCO 2900XL	11	A Switch de Jefatura							4	
SW3	SW CISCO 2900XL	12	A Switch de Poliducto Q-A-R							4	

SW #	Switch	Puerto	Nombre de Maquina	Usuario	MAC	Departamento	Unidad	Ext. IP	MAC del Telef.	VLAN Nativa	VLAN acceso
SW4	SW DLINK(5puertos)		BSQGC		00-02-A5-36-A6-E9	Sucursal Quito (Comercializadora)	Abastecedora				
SW4	SW DLINK(5puertos)		BSQAC		00-08-02-21-9A-B9	Sucursal Quito (Comercializadora)	Abastecedora				
SW5	SW DLINK (8puertos)		TPQAES	Azucena Espinoza	00-09-6B-BA-37-7B	Superint. Poliducto Q-A-R	Superint. Poliducto Quito-Ambato-Riobamba	111	08-00-0F-0E-74-3B		
SW5	SW DLINK (8puertos)		QOPISI		00-09-6B-BA-32-E8	Operaciones P. Q-A-R (Est. Bombeo)	Superint. Poliducto Quito-Ambato-Riobamba				
SW5	SW DLINK (8puertos)		QARWJ - (Prestamo de Tele.)	Mtto. De Linea de .P Q-A-R	00-10-60-76-7D-F1	Mtto. De Linea de .P Q-A-R	Superint. Poliducto Quito-Ambato-Riobamba	389	08-00-0F-0E-73-39		
SW5	SW DLINK (8puertos)		TPQMM	Ing. Mena	00-0D-9D-5D-8E-7D	Superint. Poliducto Q-A-R	Superint. Poliducto Quito-Ambato-Riobamba				
SW6	SW DLINK(5puertos)		GPIJM (Portatil)		00-0E-7F-7B-E7-B5	Protección Ambiental	Protec. Ambiental y Seguridad Industrial				
SW6	SW DLINK(5puertos)		GPICS		00-02-55-5D-B8-C2	Seguridad Industrial	Protec. Ambiental y Seguridad Industrial				
SW6	SW DLINK(5puertos)		GPICS2		XX-XX-XX-49-5F-C7	Seguridad Industrial	Protec. Ambiental y Seguridad Industrial				
SW6	SW DLINK (5puertos)		PSI04	Germania Flores	00-05-5D-2A-CC-B3	Seguridad Industrial	Protec. Ambiental y Seguridad Industrial	114	08-00-0F-01-B7-88		
SW7	SW CNET (8puertos)		EEBEL		00-02-A5-36-A7-33	Reductora	Superint. Poliducto Esm-StoDmgo-Quito-Mac				
SW7	SW CNET(8puertos)			Operadores		Reductora	Superint. Poliducto Esm-StoDmgo-Quito-Mac	126	08-00-0F-05-15-B3		
SW7	SW 3COM (8puertos)		BBT74		00-8100-80-A6-9C	Bodega	Materiales				
SW7	SW 3COM (8puertos)		QBB21	Jorge Jaramillo	00-09-6B-BA-34-04	Bodega	Materiales	115	08-00-0F-05-15-AA		
SW8	SW CNET (8puertos)		Lab1	Edgar Padilla	00-10-B5-72-F0-B5	Lab. Control de Calidad	Superintendencia de Terminales y Depósitos	5113	08-00-0F-0E-66-CC		
SW8	SW CNET (8puertos)		YCCPJ		00-02-55-5D-BA-11	Lab. Control de Calidad	Superintendencia de Terminales y Depósitos				
SW9	SW DLINK(8puertos)		PJC-02		00-02-3F-80-A1-8B	Mtto. Eléctrico (Portatil)	Superintendencia de Terminales y Depósitos				
SW9	SW DLINK(8 puertos)		NN		00-10-5A-4A-99-ED	Mtto. Industrial	Superintendencia de Terminales y Depósitos				
SW9	SW DLINK(8 puertos)			Pamela	00-0F-B0-40-8F-AE	Mtto. Eléctrico (Portatil)	Superintendencia de Terminales y Depósitos				

ANEXO 16: Configuración y Verificación de los Equipos de Beaterio

Configuración del Switch de Telecomunicaciones (172.20.129.1)

```
BIENVENIDOS AL SWITCH DE TELECOMUNICACIONES

User Access Verification

Password:
Password:
Telecom>en
Password:
Password:
Telecom#sh run
Building configuration...

Current configuration : 4501 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Telecom
!
enable secret 5 xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
enable password cisco
!
ip subnet-zero
ip routing
ip host Sucursal 172.20.129.3
ip host Jefatura 172.20.129.2
!
mls qos
cluster enable Beaterio 0
cluster member 1 mac-address 000a.f4f2.bc00
cluster member 2 mac-address 0004.c1aa.4440
!
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 2 priority 24576
spanning-tree vlan 3 priority 24576
spanning-tree vlan 4 priority 24576
!
!
interface FastEthernet0/1
 description Conexion al Router Motorola (220)
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/2
 description Conexion a Netbuffer de Central
 switchport access vlan 4
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/3
 description Conexion a la Central IP Mitel
 switchport access vlan 3
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/4
```

```
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/5
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/6
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust cos
 spanning-tree portfast
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
 mls qos trust cos
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/10
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/11
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/12
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
 no ip address
 mls qos trust cos
 spanning-tree portfast
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
 no ip address
 mls qos trust cos
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/17
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport voice vlan 4
```

```
 no ip address
 mls qos trust cos
 spanning-tree portfast
!
interface FastEthernet0/19
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/20
 switchport access vlan 4
 no ip address
!
interface FastEthernet0/21
 description PRUEBA
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport voice vlan 3
 no ip address
 spanning-tree portfast
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 2
 switchport mode trunk
 no ip address
!
interface FastEthernet0/23
 description Conexion a Mtto Electrico
 switchport access vlan 2
 switchport mode access
 no ip address
!
interface FastEthernet0/24
 description Conexion a Jet-Fuel
 switchport access vlan 2
 switchport mode access
 no ip address
!
interface GigabitEthernet0/1
 description Conexion al Switch de Jefaura
 switchport trunk encapsulation dot1q
 switchport mode trunk
 no ip address
!
interface GigabitEthernet0/2
 no ip address
!
interface Vlan1
 ip address 172.20.129.1 255.255.255.224
 ip helper-address 172.20.129.70
!
interface Vlan2
 ip address 172.20.129.33 255.255.255.224
 ip helper-address 172.20.129.70
!
interface Vlan3
 ip address 172.20.129.65 255.255.255.192
!
interface Vlan4
 ip address 172.20.129.129 255.255.255.128
 ip helper-address 172.20.129.70
!
router rip
 version 2
 network 172.20.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.20.129.11
ip http server
!
ip access-list standard Automatizacion
 deny   172.20.129.64 0.0.0.63
 deny   172.20.129.128 0.0.0.127
 deny   172.20.129.0 0.0.0.31
 permit any
!
```

```
ip access-list extended CMP-NAT-ACL
 dynamic Cluster-HSRP deny   ip any any
 dynamic Cluster-NAT permit ip any any
!
!
banner motd ^CBIENVENIDOS AL SWITCH DE TELECOMUNICACIONES^C
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password xxxxxx
 login
line vty 5 15
 password xxxxxx
 login
!
end

Telecom#
```

Configuración del Switch de Jefatura (172.20.129.2)

```
BIENVENIDOS AL SWITCH  DE JEFATURA

User Access Verification

Password:
Jefatura>en
Password:
Jefatura#sh run
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Jefatura
!
enable secret 5 $1$qz5T$hav1I.8NtAlDeskhkpHM70
!
!
!
!
!
!
ip subnet-zero
ip host Sucursal 172.20.129.3
ip host Telecom 172.20.129.1
!
cluster commander-address 000d.bd97.7100 member 1 name Beaterio
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 4
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 4
!
interface FastEthernet0/5
```

```
 switchport access vlan 4
!
interface FastEthernet0/6
 switchport access vlan 4
!
interface FastEthernet0/7
 switchport access vlan 4
!
interface FastEthernet0/8
 switchport access vlan 4
!
interface FastEthernet0/9
 switchport access vlan 4
!
interface FastEthernet0/10
 switchport access vlan 4
!
interface FastEthernet0/11
 switchport access vlan 4
!
interface FastEthernet0/12
 switchport access vlan 4
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/14
 description Conexion al Switch de Sucursal
 duplex full
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/15
 switchport access vlan 4
!
interface FastEthernet0/16
 description Conexion al Switch de Bodega
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/18
 switchport access vlan 4
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/22
 description Conexion al Switch de Control de Calidad
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
```

```
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface VLAN1
 ip address 172.20.129.2 255.255.255.224
 no ip directed-broadcast
 ip nat outside
 no ip route-cache
!
ip default-gateway 172.20.129.1
snmp-server engineID local 000000090200000A8A4CCBC0
snmp-server community private RW
snmp-server community public RO
banner motd ^CBIENVENIDOS AL SWITCH  DE JEFATURA^C
!
line con 0
 password cisco
 login
 transport input none
 stopbits 1
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end

Jefatura#
```

Configuración del Switch de Sucursal (172.20.129.3)

```
BIENVENIDOS AL SWITH DE SUCURSAL-COMERCIALIZADORA

User Access Verification

Password:
Sucursal>en
Password:
Sucursal#sh run
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Sucursal
!
enable secret 5 $1$qz5T$hav1I.8NtAlDeskhkpHM70
!
!
!
!
!
!
ip subnet-zero
ip host Telecom 172.20.129.1
ip host Jefatura 172.20.129.2
!
```

```
cluster commander-address 000d.bd97.7100 member 2 name Beaterio
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface FastEthernet0/10
 switchport access vlan 4
!
interface FastEthernet0/11
 description Conexion al Switch de Jefatura
 duplex full
 speed 100
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/12
 description Conexion al Switch de Poliducto Q-A-R
 duplex full
 speed 100
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 4
 switchport mode trunk
!
interface VLAN1
 ip address 172.20.129.3 255.255.255.224
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 172.20.129.1
snmp-server engineID local 0000000902000004C1AA4440
snmp-server community private RW
snmp-server community public RO
banner motd ^CBIENVENIDOS AL SWITH DE SUCURSAL-COMERCIALIZADORA^C
```

```
!
line con 0
 password cisco
 transport input none
 stopbits 1
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end

Sucursal#
```

Configuración de VTP del Switch de Telecomunicaciones (172.20.129.1)

```
Telecom#sh vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : BeaterioVTP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA2 0x40 0x7F 0x54 0xA9 0xA5 0x76 0xA5
Configuration last modified by 172.20.129.1 at 3-20-93 00:53:51
Local updater ID is 172.20.129.1 on interface Vl1 (lowest numbered VLAN interfac
e found)
```

Configuración de VTP del Switch de Jefatura (172.20.129.2)

```
Jefatura#sh vtp st
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 254
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : BeaterioVTP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA2 0x40 0x7F 0x54 0xA9 0xA5 0x76 0xA5
Configuration last modified by 172.20.129.1 at 3-20-93 00:53:51
Jefatura#
```

Configuración de VTP del Switch de Sucursal (172.20.129.3)

```
Sucursal
Sucursal#sh vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 68
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : BeaterioVTP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA2 0x40 0x7F 0x54 0xA9 0xA5 0x76 0xA5
Configuration last modified by 172.20.129.1 at 3-20-93 00:53:51
Sucursal#
```

Tabla de Enrutamiento del Switch de Telecomunicaciones (172.20.129.1)

```
Telecom#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is 172.20.129.11 to network 0.0.0.0

     172.17.0.0/24 is subnetted, 2 subnets
R       172.17.28.0 [120/3] via 172.20.129.11, 00:00:04, Vlan1
R       172.17.16.0 [120/3] via 172.20.129.11, 00:00:04, Vlan1
R    172.16.0.0/16 [120/2] via 172.20.129.11, 00:00:04, Vlan1
R    172.19.0.0/16 [120/2] via 172.20.129.11, 00:00:04, Vlan1
     172.20.0.0/16 is variably subnetted, 67 subnets, 7 masks
R       172.20.36.156/30 [120/2] via 172.20.129.11, 00:00:04, Vlan1
R       172.20.36.152/30 [120/2] via 172.20.129.11, 00:00:04, Vlan1
R       172.20.169.0/24 [120/4] via 172.20.129.11, 00:00:04, Vlan1
R       172.20.170.0/26 [120/4] via 172.20.129.11, 00:00:04, Vlan1
R       172.20.171.0/26 [120/2] via 172.20.129.11, 00:00:04, Vlan1
R       172.20.36.136/30 [120/2] via 172.20.129.11, 00:00:04, Vlan1
R       172.20.36.132/30 [120/2] via 172.20.129.11, 00:00:04, Vlan1
R       172.20.161.0/24 [120/3] via 172.20.129.11, 00:00:04, Vlan1
C       172.20.129.32/27 is directly connected, Vlan2
R       172.20.162.0/24 [120/3] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.163.0/24 [120/2] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.164.0/24 [120/3] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.36.128/30 [120/2] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.165.0/26 [120/4] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.165.0/24 [120/3] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.167.0/26 [120/4] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.136.0/24 [120/3] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.137.0/24 [120/3] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.138.0/24 [120/3] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.139.0/24 [120/2] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.36.168/30 [120/2] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.140.0/24 [120/2] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.36.164/30 [120/2] via 172.20.129.11, 00:00:06, Vlan1
C       172.20.129.0/27 is directly connected, Vlan1
R       172.20.130.0/24 [120/4] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.131.0/24 [120/2] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.36.160/30 [120/2] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.132.0/24 [120/2] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.133.0/24 [120/3] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.134.0/24 [120/3] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.170.64/26 [120/4] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.165.64/26 [120/3] via 172.20.129.11, 00:00:06, Vlan1
R       172.20.167.64/26 [120/4] via 172.20.129.11, 00:00:07, Vlan1
C       172.20.129.64/26 is directly connected, Vlan3
R       172.20.36.28/30 [120/1] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.39.28/30 [120/3] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.24/30 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.39.24/30 [120/3] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.20/30 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.16/30 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.12/30 [120/1] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.170.128/26 [120/4] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.8/30 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.40.4/30 [120/3] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.39.8/30 [120/3] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.4/30 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.0/30 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.167.128/26 [120/4] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.60/30 [120/4] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.56/30 [120/4] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.52/30 [120/3] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.48/30 [120/4] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.44/30 [120/3] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.40/30 [120/3] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.36/30 [120/4] via 172.20.129.11, 00:00:07, Vlan1
C       172.20.129.128/25 is directly connected, Vlan4
R       172.20.32.92/30 [120/3] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.170.192/26 [120/4] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.68/30 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.97.0/24 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.36.64/30 [120/4] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.40.96/27 [120/3] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.75.0/24 [120/2] via 172.20.129.11, 00:00:07, Vlan1
```

```
R       172.20.64.11/32 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.76.0/24 [120/3] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.77.0/24 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       172.20.64.0/21 [120/2] via 172.20.129.11, 00:00:07, Vlan1
    10.0.0.0/24 is subnetted, 2 subnets
R       10.10.10.0 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       10.1.7.0 [120/2] via 172.20.129.11, 00:00:07, Vlan1
    200.24.212.0/24 is variably subnetted, 2 subnets, 2 masks
R       200.24.212.21/32 [120/2] via 172.20.129.11, 00:00:07, Vlan1
R       200.24.212.16/29 [120/2] via 172.20.129.11, 00:00:07, Vlan1
S*   0.0.0.0/0 [1/0] via 172.20.129.11
Telecom#
```

Configuración de la Interfaz LAN del Router Vanguard Motorota

Configure IP Parameters

```
*Maximum Number of IP Interfaces: 36/
Internal IP Address: (blank)/
Internal Net Mask: 255.255.255.0/
Access Control: Disabled/
RIP Enable: Enabled/
Originate Default Route: Disabled/
Advertised Default Route Metric: 10/
Default Gateway: 0.0.0.0/
Default Gateway Metric: 10/
Directed Broadcast: Enabled/
All Subnet Broadcast: Disabled/
*IP Route Table Size: 768/
*IP Route Cache Size: 64/
*Reassembly Buffer Size: 12000/
BOOTP Forwarding: Enabled/
BOOTP Max Allowed Metric: 4/
BOOTP Seconds Before Forward: 0/
IP Broadcast Forwarding Enable: Disabled/
UDP Broadcast Forwarding Enable: Disabled/
*Aggregated Cache Enable: Enabled/
Source Address Options: Default/
BGP to RIP Enable: Disabled/
BGP to RIP Default Filter: Deny/
BGP to RIP Nondefault Route Override: Disable/
BGP to RIP Default Route Override: Disable/
BGP to RIP Default Metric: 1/
```

Configure IP Interface Configuration Table

```
Entry Number: 1/
[1] Interface Number: 1/
[1] IP Address : 172.20.129.11/
[1] IP Address Mask: 255.255.255.0/
[1] Accept RIP: VER2/
[1] RIP metric: 1/
[1] Send RIP Version: VER2_M/
[1] Send Aggregated Routes: Disabled/
[1] Authentication Type: None/
[1] Periodic Broadcast Interval: 30/
[1] Route Invalid Time: 180/
[1] Route Flush Time: 300/
[1] Route Hold Down Time: 240/
[1] Learn Network Routes: Enabled/
[1] Learn Subnet Routes: Enabled/
[1] Override Default Route: Disabled/
[1] Override Static Routes: Disabled/
[1] Advertise Default Route: Disabled/
[1] Advertise Network Routes: Enabled/
[1] Advertise Subnet Routes: Enabled/
[1] Advertise Static Routes: Enabled/
[1] Advertise Direct Routes: Enabled/
[1] IP RIP Split Horizon: With_Poison_Reverse/
[1] Broadcast Style: LOCAL/
[1] Broadcast Fill Pattern: 1/
[1] MTU Size: 1500/
```

[1] Duplicate Address Detection: Disabled/
[1] VLAN ID: 1/
[1] Default Ethernet Priority: 0/
[1] Send IP Redirect: Enabled/
[1] PIM Mode: None/
[1] Interface Number: 1/

Configure Port

Port Number: 6/5
[5] *Port Type: ETH/
[5] *Port MAC Address: 00-00-00-00-00-00/
[5] Transmit Queue Limit: 50/
[5] Carrier Sense Filter: 0/
[5] Collision Detect Filter: 0/
[5] *Bridge Link Number: 1/
[5] *Router Interface Number: 1/
[5] VLAN Encapsulation: None/
[5] DSCP-to-CoS Profile: 0/

Tabla de Enrutamiento del Router Vanguard Motorola (220)

Node: BEATER_A Address: 220 Date: 31-MAR-2005 Time: 14:54:
IP Routing Table

* Static/Direct Route
% RIP Route Control

Type	Dest net	Mask	Metric	Age	Next hop
Sbnt	10.0.0.0	ff000000	1	0	None
RIP	10.1.7.0	ffffff00	2	30	172.20.36.13
RIP	10.10.10.0	ffffff00	2	30	172.20.36.13
RIP	172.16.0.0	ffff0000	2	30	172.20.36.13
Sbnt	172.17.0.0	ffff0000	1	0	None
RIP	172.17.16.0	ffffff00	3	30	172.20.36.13
RIP	172.17.28.0	ffffff00	3	30	172.20.36.13
RIP	172.19.0.0	ffff0000	2	30	172.20.36.13
Sbnt	172.20.0.0	ffff0000	1	0	None
RIP	172.20.32.92	fffffffc	3	30	172.20.36.13
RIP	172.20.36.0	fffffffc	2	30	172.20.36.13
RIP	172.20.36.4	fffffffc	2	30	172.20.36.13
RIP	172.20.36.8	fffffffc	2	30	172.20.36.13
Dir	172.20.36.12	fffffffc	1	0	SL/5
RIP	172.20.36.16	fffffffc	2	30	172.20.36.13
RIP	172.20.36.20	fffffffc	2	30	172.20.36.13
RIP	172.20.36.24	fffffffc	2	30	172.20.36.13
Dir	172.20.36.28	fffffffc	1	0	SL/6
RIP	172.20.36.36	fffffffc	4	30	172.20.36.13
RIP	172.20.36.40	fffffffc	3	30	172.20.36.13
RIP	172.20.36.44	fffffffc	3	30	172.20.36.13
RIP	172.20.36.48	fffffffc	4	30	172.20.36.13
RIP	172.20.36.52	fffffffc	3	30	172.20.36.13
RIP	172.20.36.56	fffffffc	4	30	172.20.36.13
RIP	172.20.36.60	fffffffc	4	30	172.20.36.13
RIP	172.20.36.64	fffffffc	4	30	172.20.36.13
RIP	172.20.36.68	fffffffc	2	30	172.20.36.13
RIP	172.20.36.128	fffffffc	2	30	172.20.36.13
RIP	172.20.36.132	fffffffc	2	30	172.20.36.13
RIP	172.20.36.136	fffffffc	2	30	172.20.36.13
RIP	172.20.36.152	fffffffc	2	30	172.20.36.13
RIP	172.20.36.156	fffffffc	2	30	172.20.36.13
RIP	172.20.36.160	fffffffc	2	30	172.20.36.13
RIP	172.20.36.164	fffffffc	2	30	172.20.36.13
RIP	172.20.36.168	fffffffc	2	30	172.20.36.13
RIP	172.20.39.8	fffffffc	3	30	172.20.36.13
RIP	172.20.39.24	fffffffc	3	30	172.20.36.13
RIP	172.20.39.28	fffffffc	3	30	172.20.36.13
RIP	172.20.40.4	fffffffc	3	30	172.20.36.13
RIP	172.20.40.96	ffffffe0	3	30	172.20.36.13
RIP	172.20.64.0	fffff800	2	30	172.20.36.13
RIP	172.20.64.11	ffffffff	2	30	172.20.36.13

```
 RIP   172.20.75.0      ffffff00  2         30   172.20.36.13
 RIP   172.20.76.0      ffffff00  3         30   172.20.36.13
 RIP   172.20.77.0      ffffff00  2         30   172.20.36.13
 RIP   172.20.97.0      ffffff00  2         30   172.20.36.13
 Dir   172.20.129.0     ffffff00  1         0    ETH/1
 RIP   172.20.129.32    fffffffe0  2        10   172.20.129.1
 RIP   172.20.129.64    ffffffc0  2         10   172.20.129.1
 RIP   172.20.129.128   ffffff80  2         10   172.20.129.1
 RIP   172.20.130.0     ffffff00  4         30   172.20.36.13
 RIP   172.20.131.0     ffffff00  2         30   172.20.36.13
 RIP   172.20.132.0     ffffff00  2         30   172.20.36.13
 RIP   172.20.133.0     ffffff00  3         30   172.20.36.13
 RIP   172.20.134.0     ffffff00  3         30   172.20.36.13
 RIP   172.20.136.0     ffffff00  3         30   172.20.36.13
 RIP   172.20.137.0     ffffff00  3         30   172.20.36.13
 RIP   172.20.138.0     ffffff00  3         30   172.20.36.13
 RIP   172.20.139.0     ffffff00  2         30   172.20.36.13
 RIP   172.20.140.0     ffffff00  2         30   172.20.36.13
 RIP   172.20.161.0     ffffff00  3         30   172.20.36.13
 RIP   172.20.162.0     ffffff00  3         30   172.20.36.13
 RIP   172.20.163.0     ffffff00  2         30   172.20.36.13
 RIP   172.20.164.0     ffffff00  3         30   172.20.36.13
 RIP   172.20.165.0     ffffff00  3         30   172.20.36.13
 RIP   172.20.165.0     ffffffc0  4         30   172.20.36.13
 RIP   172.20.165.64    ffffffc0  3         30   172.20.36.13
 RIP   172.20.167.0     ffffffc0  4         30   172.20.36.13
 RIP   172.20.167.64    ffffffc0  4         30   172.20.36.13
 RIP   172.20.167.128   ffffffc0  4         30   172.20.36.13
 RIP   172.20.169.0     ffffff00  4         30   172.20.36.13
 RIP   172.20.170.0     ffffffc0  4         30   172.20.36.13
 RIP   172.20.170.64    ffffffc0  4         30   172.20.36.13
 RIP   172.20.170.128   ffffffc0  4         30   172.20.36.13
 RIP   172.20.170.192   ffffffc0  4         30   172.20.36.13
 RIP   172.20.171.0     ffffffc0  2         30   172.20.36.13
Sbnt   200.24.212.0     ffffff00  1         0    None
 RIP   200.24.212.16    fffffff8  2         30   172.20.36.13
 RIP   200.24.212.21    ffffffff  2         30   172.20.36.13

Routing table currently uses 79 of the 768 routes available.
```

ÍNDICE DE FIGURAS

FIGURAS DEL CAPITULO I: **Pág.**

FIGURAS DEL CAPITULO II:

FIGURAS DEL CAPITULO III:

FIGURAS DEL CAPITULO IV:

FIGURAS DEL CAPITULO V:

ÍNDICE DE TABLAS

TABLAS DEL CAPITULO I: **Pág.**

TABLAS DEL CAPITULO II:

TABLAS DEL CAPITULO III:

TABLAS DEL CAPITULO IV:

ELABORADO POR:

Alex Homero Rivadeneira Erazo.

AUTORIDADES:

Sr. TCRN. Ing. Marcelo Gómez.
Decano de la Facultad de Ingeniería Electrónica.

Sr. Dr. Jorge Carvajal.
Secretario Académico de la Facultad de Ingeniería Electrónica.