ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA INFORMÁTICA

DISEÑO E IMPLEMENTACIÓN DE LA RED DE CAMPUS DEL MINISTERIO DE AGRICULTURA Y GANADERÍA

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO INFORMÁTICO MENCIÓN REDES DE LA INFORMACIÓN

LÓPEZ CARRERA RICARDO ARMANDO
cieguito66@hotmail.com

DIRECTOR: ING. PATRICIO PROAÑO
pproano@epn.edu.ec

Quito, Septiembre 2007

DECLARACIÓN

Yo Ricardo Armando López Carrera declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Ricardo López C.

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Ricardo Armando López Carrera, bajo mi supervisión.

ING. PATRICIO PROAÑO
DIRECTOR DE PROYECTO

DEDICATORIA

A Dios por haberme dado la fortaleza y tenacidad para poder superar todas las dificultades y poder cumplir un objetivo más de los trazados en mi vida.

Ricky Lpz.

AGRADECIMIENTO

Recibid de mi (hoy Ricky, mañana quién sabe) mi más sincero agradecimiento, en forma de reverencia virtual.

Ciertamente hay en el mundo pocos objetivos más dignos que ser tan grande como el más pequeño de mis semejantes (¡oh, don del cielo!).

GRACIAS, nobles gentes. Dios mediante, recibiréis nuevas acerca de mi éxito o, si así lo dispone la Divina Providencia, de mi fracaso.

Ricky Lpz.

CONTENIDO

CAPITULO 1

ANÁLISIS DE LA RED DE DATOS Y DE LOS REQUERIMIENTOS DEL MAG Y SUS DEPENDENCIAS.

1.1 Introducción 2
1.2 Metodología 4
1.2.1 Modularidad en SAFE 5
1.2.1.1 Campus Empresarial 6
1.2.1.2 Perímetro Empresarial 7
1.2.1.3 Proveedor de servicios perimetrales 8
1.3 Análisis y equipamiento de las redes actuales del MAG 8
1.3.1 Descripción orgánico-funcional del MAG 9
1.3.2 Estructura administrativa del MAG 11
1.3.3 Descripción de las redes de datos 12
1.3.3.1 Tecnología y topologías de las redes del MAG y sus dependencias 12
1.3.3.2 Sistema de cableado estructurado del MAG y sus dependencias..... 14
1.3.3.3 Equipamiento de las redes del MAG y sus dependencias 15
1.3.3.4 Inventario de las aplicaciones existentes 28
1.4 Requerimientos de la red del MAG 32
1.4.1 Requerimientos de tráfico de la red 32
1.4.2 Requerimientos de seguridad en la red..... 36
1.4.3 Servicios de red requeridos 37
1.4.3.1 Servicios de Internet 37
1.4.3.2 Servicios de Intranet 39
1.4.3.3 Servicio de acceso remoto (RAS)..... 40
1.5 Proyecciones y perspectivas 40

CAPITULO 2

DISEÑO DE LA RED DE CAMPUS EN TRES CAPAS DEL MAG.

2.1 Diseño de la red de campus en tres capas..... 45
2.1.1 Introducción 45
2.1.2 La tecnología IEEE 802.3 46
2.1.3 Objetivos para el diseño de la red 46
2.1.4 Consideraciones para el diseño de una red..... 47
2.1.4.1 Función y ubicación de servidores 47
2.1.4.2 Dominios de colisión..... 48
2.1.4.3 Segmentación 48
2.1.4.4 Dominio de broadcast 49
2.1.5 Aplicación de la metodología SAFE en el diseño de la red del MAG..... 50
2.1.5.1 Modelo de diseño jerárquico 50
2.1.5.1.1 Capa de acceso 50
2.1.5.1.2 Capa de distribución 51
2.1.5.1.3 Capa núcleo 53
2.1.5.2 Diseño lógico 54
2.1.6 Diseño de seguridad 57
2.2 Diseño de Vlan´s..... 59
2.2.1 Concepto de Vlan..... 59
2.2.2 Características principales 59
2.2.3 Formas de implementación de Vlan´s 59
2.2.4 Mecanismos de enlace entre Vlan´s 60
2.2.5 Control de flujo entre Vlan´s 60
2.2.6 Diseño de Vlans 61
2.3 Especificaciones de direccionamiento IP 62
2.3.1 Direccionamiento IP 62
2.3.2 Clases de direcciones IP 63
2.3.3 Máscara de red 65
2.3.4 Asignación de IP´s al Ministerio 66
2.4 Especificaciones de subred 67
2.4.1 Definiciones Básicas 67
2.4.2 Definición de subredes para el Ministerio 70
2.5 Especificaciones de enrutamiento 71
2.5.1 Enrutamiento estático o no adoptivo 71

2.5.2 Enrutamiento dinámico o adaptivo 72
2.5.3 Enrutamiento del ministerio 72
2.6 Alternativas de tecnologías para la implementación de la infraestructura WAN 73
2.6.1 Definición de los enlaces WAN con Frame Relay 80
2.6.2 Costos 80
2.6.2.1 Estructura tarifaria del servicio FR en el Ecuador 81
2.6.3 Equipos de interconexión 85

CAPITULO 3

IMPLEMENTACIÓN DE LA RED DE CAMPUS EN TRES CAPAS DEL MAG.

3.1 Implementación de equipos 88
3.1.1 Capa de acceso 89
3.1.2 Capa de distribución 90
3.1.3 Capa núcleo 91
3.1.4 Seguridad 93
3.2 Distribución de cableado y equipos 96
3.2.1 Consideraciones de construcción para el cableado estructurado 96
3.3 Configuración de equipos Cisco 106
3.3.1 Ingreso a la configuración en equipos Cisco 106
3.3.2 Uso del Command-line interface 108
3.3.3 Configuración de Password 111
3.3.4 Configuración del nombre del dispositivo 111
3.3.5 Configuración de una dirección IP 112
3.3.6 Configuración de interfases 112
3.3.7 Verificación de la configuración 113
3.3.8 Borrar la configuración 113
3.3.9 Configuración de VTP 113
3.4 Implementación de Vlan´s 114
3.4.1 Configuración de Vlan´s..... 114
3.4.2 Configuración de puertos troncales 116
3.4.3 Configuraciones de los switches del MAG 118

3.4.4 Configuración de los routers Cisco 121
3.5 Análisis de costos 123

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES.

4.1 Conclusiones 127
4.2 Recomendaciones 129

BIBLIOGRAFÍA 131

GLOSARIO DE TÉRMINOS 132

ANEXOS

INDICES DE TABLAS

Tabla 1.1 Tecnología y topología de la red del MAG y sus dependencias..... 14
Tabla 1.2 Número de puntos de red en todo el Ministerio..... 27
Tabla 1.3 Tráfico de datos en todas las redes del Ministerio..... 32
Tabla 1.4 Subsecretarías y sus Direcciones Provinciales 37
Tabla 1.5 Cantidad de equipos en las Direcciones Provinciales 38
Tabla 2.1 Aspectos de una red LAN 45
Tabla 2.2 Cantidad de IDF´s y Switchs en la capa de Acceso 51
Tabla 2.3 Cantidad de IDF´s y Switchs en la capa de Distribución 52
Tabla 2.4 Cuadro de requerimientos de la red del Ministerio 54
Tabla 2.5 Resumen del diseño de la red del Ministerio 54
Tabla 2.6 Identificación de cables de backbone..... 56
Tabla 2.7 Identificación en los puertos del HCC y los VCC 56
Tabla 2.8 Primera distribución de VLAN´s 62
Tabla 2.9 Rango de direcciones IP Privadas 63
Tabla 2.10 Clases de redes y sus valores 65
Tabla 2.11 Direcciones de red de las VLAN´s 67

Tabla 2.12 Resumen de las tecnologías analizadas ……. 80
Tabla 2.13 Derecho de inscripción para circuitos Frame Relay ……. 81
Tabla 2.14 Tarifas mensuales para circuitos Frame Relay ……. 81
Tabla 2.15 Derecho de inscripción para las Subsecretarías …….. 82
Tabla 2.16 Derecho de inscripción para las Direcciones Provinciales ……. 82
Tabla 2.17 Tarifa mensual FR para las Subsecretarías ……. 83
Tabla 2.18 Tarifa mensual FR para las Direcciones Provinciales ……. 83
Tabla 3.1 Análisis comparativo con otras marcas 88
Tabla 3.2 Características generales de Switchs Capa de Acceso ……. 89
Tabla 3.3 Número de Switchs en la capa de Acceso …….. 90
Tabla 3.4 Total de Switchs en la capa de Acceso ……. 90
Tabla 3.5 Número de Switchs en la Capa de Distribución …….. 91
Tabla 3.6 Normas internacionales para Cableado Estructurado ……. 96
Tabla 3.7 Numero de puntos por cada IDF ……. 97
Tabla 3.8 Cantidad de rollos para los puntos adicionales ……... 99
Tabla 3.9 Dimensionamiento de racks para el Ministerio……. 101
Tabla 3.10 Cantidad de elementos en los IDF´s …….. 102
Tabla 3.11 Valores de VLAN´s a configurar …….. 118
Tabla 3.12 Costos de Cableado Estructurado Cat 5e ……. 123
Tabla 3.13 Costos de Elementos Activos …….. 124
Tabla 3.14 Costos por servicios profesionales ……. 125
Tabla 3.15 Costo total del proyecto 125

INDICES DE FIGURAS

Figura 1.1 Diagrama en bloques del Módulo de Red Empresarial de SAFE ... 5
Figura 1.2 Diagrama en bloques mas detallados del Módulo de Red Empresarial de SAFE ……. 5
Figura 1.3 Diagrama en bloques del Campus Empresarial ……. 6
Figura 1.4 Organigrama estructural del MAG ……. 11
Figura 1.5 Esquema de la red física de la Administración del MAG ……. 15
Figura 1.6 Esquema de la red física del PRAT ……. 20
Figura 1.7 Esquema de la red física del SESA ……. 21

Figura 1.8 Esquema de la red física del CADERS …….. 22
Figura 1.9 Esquema de la red física del INCCA 24
Figura 1.10 Esquema de la red física del INIAP …….. 25
Figura 1.11 Esquema de la red física del CNRH ……. 26
Figura 1.12 Tráfico medido en la Administración Central del MAG 29
Figura 1.13 Resumen del tráfico medido en la Administración Central del MAG ……. 29
Figura 1.14 Tráfico medido en el CNRH ……. 31
Figura 2.1 Protocolos LAN y modelo de referencia OSI …….. 46
Figura 2.2 Dominios de Colisión y Dominios de Broadcast ……. 50
Figura 2.3 Diagrama lógico de capa 1 del Ministerio …….. 56
Figura 2.4 Diagrama físico de la red del Ministerio …….. 58
Figura 2.5 Diagrama lógico del Ministerio ……. 73
Figura 2.6 Tarifación Frame Relay ……. 78
Figura 2.7 Diagrama lógico de la interconexión entre Subsecretarías ……. 84
Figura 2.8 Distribución física de las Subsecretarías Regionales …….. 84
Figura 2.9 Distribución física de las Direcciones Provinciales ……. 85
Figura 3.1 Switch Catalyst 6006 …….. 92
Figura 3.2 Cisco ASA 5510 …….. 94
Figura 3.3 Distribución de equipos en el MAG …….. 95

RESUMEN

El presente proyecto de titulación, tiene como objetivo implementar una infraestructura de networking en el Ministerio de Agricultura y Ganadería para mejorar el desempeño de la Administración Central y la integración de sus dependencias. Esta implementación incluye un análisis de la situación actual del Ministerio, el diseño de la red y finalmente la implementación con su respectivo análisis de costos.

En el primer capítulo, se hace una descripción general de la metodología usada, se hace una descripción orgánico-funcional del ministerio, se presenta una descripción general de la arquitectura de la red de datos actual y un inventario de equipos de la administración central del MAG y sus dependencias y luego se hace un análisis de los requerimiento de tráfico y seguridad de las dependencias y de la Administración del MAG, seguido se determina los servicios de red requeridos para finalmente mencionar las proyecciones y perspectivas de interconexión con las Direcciones Provinciales como valor agregado.

A continuación en el segundo capítulo, se realiza el diseño de la red de campus en tres capas del Ministerio con sus respectivos objetivos y consideraciones aplicando la metodología SAFE, propuesta dividida en la capa de acceso, la capa de distribución y la capa núcleo, el diseño lógico, el diseño de VLAN´s y el direccionamiento IP con sus respectivas subredes y enrutamientos.

En el tercer capítulo, se realizó la implementación de la red empezando por los equipos activos utilizados en cada una de las capas y los utilizados en la seguridad, se realizó desglose del cableado estructurado pese a que este ya existía, se realizó la implementación de las VLAN´s y la configuración de los elementos activos utilizados para terminar con un análisis de costos.

Y por último en el capítulo cuarto, se describen las conclusiones y recomendaciones obtenidas en esta implementación.

PRESENTACIÓN

En la actualidad El Ministerio de Agricultura y Ganadería - MAG en su parte administrativa y sus dependencias afines como SESA, INIAP, INNCA, CNRH, PRAT y CADERS, se manejan de forma independiente y autónoma tanto administrativamente como tecnológicamente, con las últimas reformas agrarias se ha visto en la necesidad de unificar todas estas dependencias para tener un mejor control del agro ecuatoriano.

Debido a la situación económica del país, el gobierno ecuatoriano ha optado por reducir el gasto público en todas sus dependencias y Ministerios para lo cual se les ha pedido tomen los correctivos necesarios, para que dicho ahorro sea lo más significativo posible.

El Ministerio de Agricultura y Ganadería se ha visto en la necesidad de reducir su gasto tomando ciertas acciones y entre ellas está la tecnológica para optimizar recursos como la interconexión de todas sus dependencias y así no tener gastos duplicados como varias cuentas de Internet, varios centros de cómputo, mayor personal de soporte, etc. para lo cual se propone el diseño, instalación y puesta en perfecto estado de funcionamiento del equipamiento de networking para la interconexión entre las dependencias mediante una red de campus en tres capas.

Todo esto para que la Administración Central del MAG y las dependencias antes descritas sean una sola red corporativa para transmisión de datos y como consecuencia de la optimización de recursos exista un ahorro en el presupuesto de dicha cartera.

Además del ahorro económico, el MAG tendrá otra ventaja que es el disponer de información de todas sus dependencias de forma instantánea y actualizada para que así el titular de esta cartera pueda tomar las decisiones más acertadas.

CAPITULO 1

ANÁLISIS DE LA RED DE DATOS Y DE LOS REQUERIMIENTOS DEL MAG Y SUS DEPENDENCIAS.

2.1 INTRODUCCIÓN

El progresivo desarrollo y utilización de las diferentes tecnologías de comunicación ha permitido que en la actualidad sea un factor clave el manejo adecuado de la información. Debido a la multiplicación de nuevos servicios en torno a las comunicaciones, así como la expansión y dispersión de una empresa en distintas localidades geográficas, cada vez es más importante para las organizaciones disponer de una infraestructura de red capaz de soportar el tráfico de información que se genera.

El desarrollo de cualquier tipo de actividad, que a su vez se encuentra bajo una situación de cambio tecnológico permanente, requiere la implementación de una red rápida, confiable, estable, disponible, segura, escalable y que permita el acceso a los servicios corporativos desde cualquiera de los puntos operativos de la misma.

La necesidad del intercambio de información de una manera sencilla ha llevado a la implementación de redes de datos mediante la interconexión de servidores, computadores, impresoras y otros dispositivos electrónicos, mediante cables o enlaces inalámbricos que permiten la comunicación de unos con otros.

Anteriormente para implementar la red en una empresa se utilizaban sistemas independientes, tanto para la red de voz como para la red de datos, haciendo más complejo su administración y mantenimiento. En la actualidad se utilizan sistemas de cableado estructurado que permiten integrar los servicios de voz, datos y vídeo, estandarizando los sistemas de transmisión de información, además de utilizar una misma estructura de comunicación para todos los servicios que se quieran prestar, dando origen a un sistema centralizado que facilita su administración, mantenimiento, y es fácilmente ampliable. Una de las ventajas básicas de un sistema de cableado estructurado es que se encuentra regulado mediante estándares, garantizándose su funcionalidad en comunicación y transmisión de información para las distintas aplicaciones que se pueden desarrollar en ambientes corporativos.

Gracias a los actuales servicios de telecomunicaciones, se pueden tener los servicios de Internet y, a través de esta red pública, se pueden implementar servicios de VPN (Redes Privadas Virtuales) seguras, que permiten la interconexión de las diferentes dependencias de una empresa localizadas en diferentes puntos geográficos.

Mediante la implementación de una red de datos corporativa, una organización puede ser más competitiva. La red de datos permite a sus usuarios compartir e intercambiar información, acceder a servicios comunes como correo electrónico, Internet, o aplicaciones específicas, y compartir elementos de hardware como servidores, impresoras o equipos de fax. El estar conectada una organización y todas sus dependencias permitirá disponer e intercambiar información necesaria en el menor tiempo posible, logrando una mayor productividad y competitividad, factores importantes en el mundo globalizado actual.

El Ministerio de Agricultura y Ganadería posee un conjunto de redes de datos independientes y se requiere determinar su estado actual, además es necesario la modernización tecnológica de esta institución de acuerdo a los actuales avances y como parte de esto, implementar un esquema de networking, sistemas de información y servicios de red.

El Ministerio de Agricultura y Ganadería está obligado a modernizarse mediante la utilización de nueva tecnología de información, que le permita ser más competitivo y contribuir al desarrollo del Agro.

En términos generales, se requiere una interconexión de la Administración Central del MAG y sus dependencias, que permita compartir los recursos, aplicaciones y especialmente datos que estarán disponibles para los usuarios de la red de acuerdo a la organización interna de la institución, sin importar la localización de los usuarios.

2.2 METODOLOGÍA

SAFE[1] Blueprint de Cisco proporciona una metodología para el diseño e implementación de redes seguras empresariales, para la implementación se deberán tomar decisiones que dependerán de los requerimientos de funcionalidad de la red requerida. SAFE tiene una arquitectura modular que considera los siguientes objetivos de diseño:

- Seguridad y atenuación de ataques basados en políticas.
- Implementación de seguridad en toda la infraestructura.
- Administración de la seguridad.
- Autenticación y autorización de usuarios y administradores a recursos críticos de la red.
- Protección contra intrusiones con sistemas de detección de intrusos para recursos críticos y subredes en tiempo real (IDS) y herramientas de análisis de vulnerabilidad.
- Conectividad segura para las empresas que dependen de redes públicas como el Internet para comunicarse con sucursales, o usuarios móviles.
- Seguridad perimetral para controlar el acceso de usuarios autorizados.
- Escalabilidad para poder crecer sin producir cambios importantes en el diseño.

Las redes empresariales en la actualidad abren sus infraestructuras para tener conectividad a Internet, acceso remoto, permitir accesos a usuarios móviles, aplicaciones entre empresas o sucursales, lo cual les convierte en redes más vulnerables a los ataques externos. SAFE provee una guía para el diseño de una red segura mediante módulos cada uno de los cuales puede incluir firewalls, detección de intrusos y sistemas de escaneo, autenticación de usuarios, tecnologías antivirus, encriptación, VPN´s. El marco modular, escalable, permite que los administradores construyan soluciones por etapas, realizando personalizaciones para aplicaciones, entornos y usuarios específicos.

[1] http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.pdf

2.2.2 MODULARIDAD EN SAFE

El primer gran módulo de SAFE llamado Módulo de Red Empresarial y que es el que se aplicará en parte en este proyecto, se muestra en las figuras 1.1 y 1.2.

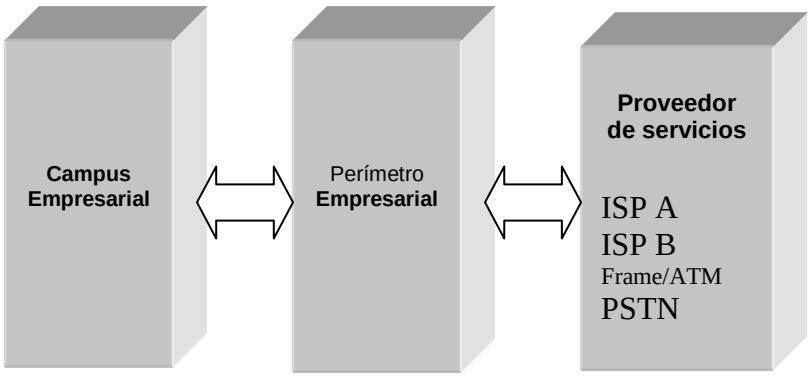


Fig. 1.1 Diagrama en bloques del Módulo de Red Empresarial de SAFE.

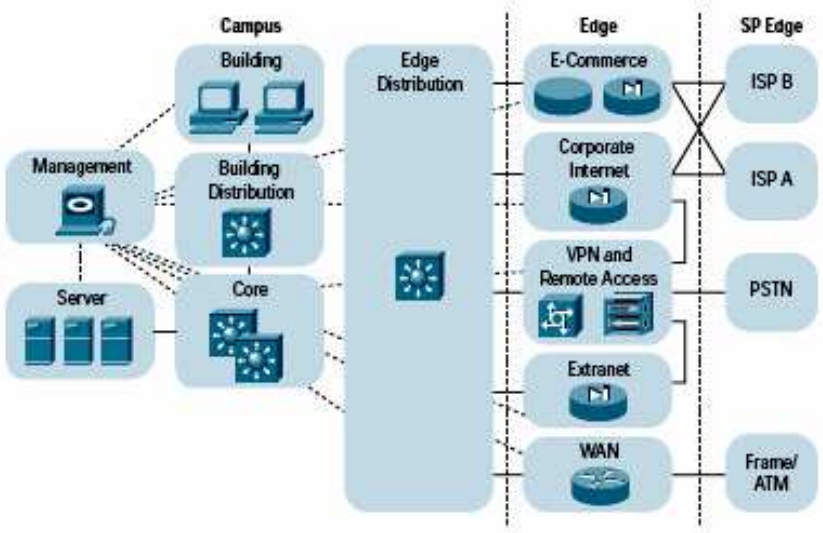


Fig. 1.2 Diagrama en bloques más detallados del Módulo de Red Empresarial de SAFE.[2]

Este módulo contiene las siguientes áreas funcionales:

- Campus Empresarial
- Perímetro Empresarial
- Proveedor de Servicios (ISP)

A continuación se describen dichas áreas:

[2] http://www.cisco.com/warp/public/cc/so/cuso/Cisco_SAFE: A Security Blueprint for Enterprise Networks

1.2.2.1 Campus Empresarial

La figura 1.3 muestra el diagrama en bloques del Campus Empresarial y a continuación se hace un análisis detallado de todos los módulos contenidos en este campus.

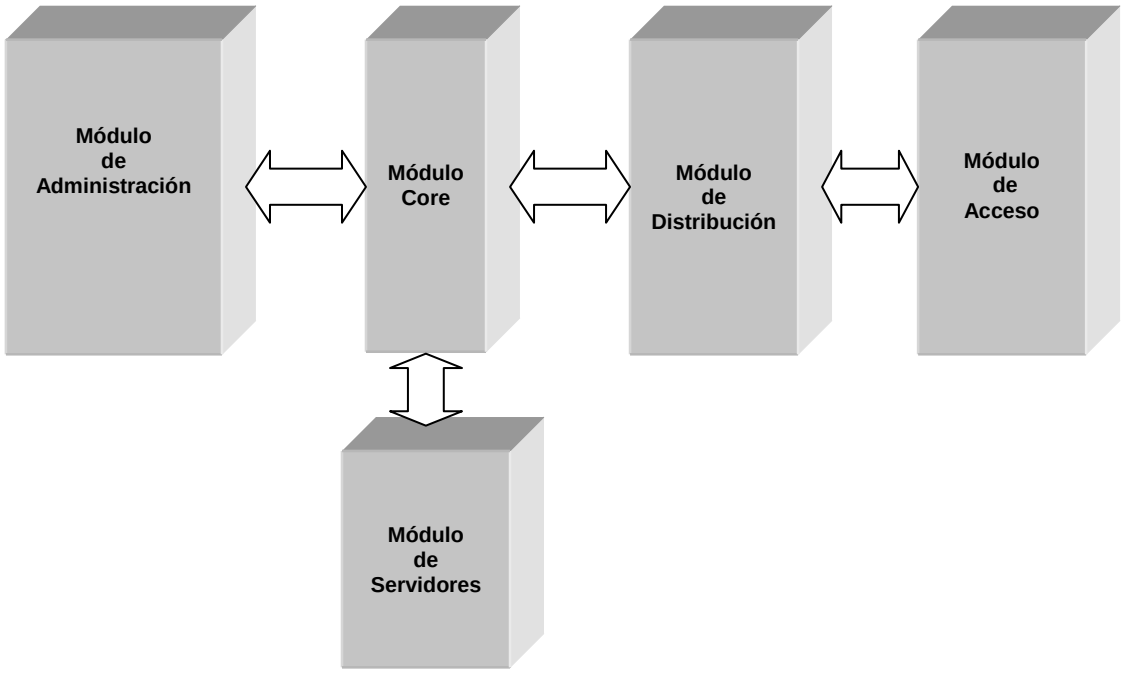


Fig. 1.3 Diagrama en bloques del Campus Empresarial

Modulo de Administración: Facilita el manejo seguro de todos los dispositivos y hosts en la estructura empresarial, en este módulo se consideran dos segmentos de red separados por un router. El primer segmento contiene todos los hosts de administración entre los cuales se puede considerar los servidores de control de acceso, monitoreo de red, sistemas de detección de intrusos, syslogs, los cuales están encargados de la administración de configuraciones, actualizaciones de software, autenticación de usuarios, monitoreo y logs. El segundo segmento conecta a todos los dispositivos que requieren administración.

Modulo Core: Es casi idéntico al módulo Core de cualquier otra arquitectura de red, este módulo está constituido por routers y switches encargados del envío de la información tan rápido como sea posible de una red hacia otra, establece la comunicación hacia el módulo de distribución de edificio y el módulo de servidores.

Módulo de Distribución: Se divide en el módulo de Distribución de Edificios y el módulo de Distribución Perimetral. El primero tiene como objetivo proveer de servicios de capa de distribución hacia los switchs de acceso que son utilizados para la conexión de usuarios finales, incluyendo ruteo, calidad de servicio (QoS) y control de acceso, este módulo provee la primera línea de defensa contra ataques originados internamente, restringiendo el acceso a ciertos departamentos de acuerdo a las políticas establecidas por la empresa.

El Módulo de Distribución Perimetral, su objetivo es incrementar la conectividad de varios elementos en el perímetro, el tráfico es filtrado y ruteado desde los módulos de la periferia y ruteado al módulo core. El módulo de Distribución Perimetral provee la última línea de defensa contra ataques. También ofrece conectividad con varios módulos contenidos en el perímetro empresarial como: comercio electrónico, Internet corporativo, VPN-acceso remoto, y WAN.

Módulo de Acceso: O módulo de edificio, se lo define como la parte de la red que contiene las estaciones de trabajo, teléfonos y todos los puntos de acceso asociados a la capa 2 del usuario final, provee servicio de datos a usuarios autorizados en la red. La seguridad debe ser implementada a nivel de workstation con algún sistema de escaneo de virus.

Módulo de Servidores: El objetivo principal del módulo de servidores es proporcionar servicios de aplicaciones para usuarios finales y dispositivos, el flujo de tráfico en este módulo puede ser controlado por switches de capa 3 y sistemas de detección de intrusos. Este módulo puede contener servidores de E-mail Interno, Servidores Departamentales, Servidores Corporativos, Call Manager y los Switchs de capa 3.

1.2.2.2 Perímetro empresarial

En este están contenidos los siguientes módulos: Módulo de Comercio Electrónico, Módulo de Internet Compartido, Módulo de VPN´s y Acceso Remoto y Módulo WAN. A continuación se realiza un análisis general de cada uno.

Módulo de Comercio Electrónico: Nombrado así porque el comercio electrónico es el objetivo principal de este módulo, el equilibrio entre acceso y

seguridad debe ser cuidadosamente medido, se divide la transacción en componentes, se permite que la arquitectura proporcione varios niveles de seguridad sin impedir el acceso.

Módulo de Internet corporativo: Este módulo proporciona a los usuarios internos de conectividad a servicios de Internet y a usuarios de Internet a información del exterior. El tráfico también fluye de este módulo al módulo de VPN´s y de acceso remoto.

Módulo de VPN´s y acceso remoto: El principal objetivo es determina el tráfico desde usuarios remotos a las VPN´s y terminar con los tradicionales usuarios Dial-up.

Módulo WAN: En lugar de tener un diseño todo incluido, este módulo resalta la seguridad en la parte final hacia la WAN. Usando encapsulamiento Frame Relay o ATM, el tráfico es ruteado entre sitios remotos y el sitio central.

1.2.2.3 Proveedor de servicios perimetrales.

El módulo Proveedor de Servicios Perimetrales no es implementado por las empresas, pero se incluyen las características de seguridad que debe seguir un proveedor de servicios para mitigar ciertos ataques.

En la red corporativa del MAG se implantará principalmente el Campus Empresarial y sus respectivos módulos, algunos módulos del Perímetro Empresarial como Internet Corporativo, VPN´s y WAN se implementarán pero no son el objetivo principal.

2.3 ANÁLISIS Y EQUIPAMIENTO DE LAS REDES ACTUALES DEL MAG.

La Administración Central del MAG y sus dependencias poseen redes de datos independientes y se requiere realizar un análisis para determinar el estado actual de dichas redes, para lo cual se empezará haciendo un inventario de las redes actuales del MAG y sus dependencias, pero antes se hará una breve descripción orgánico-funcional del ministerio.

2.3.2 DESCRIPCIÓN ORGÁNICO-FUNCIONAL DEL MAG.[3]

El marco legal de las políticas que rigen el funcionamiento del MAG están establecidos en la Constitución del Estado que, en los artículos No. 266 al 270 de manera concreta señalan: "Será objetivo permanente de las políticas del Estado el desarrollo prioritario, integral y sostenido de las actividades agrícola, pecuaria, acuícola, pesquera, agroindustrial y agroforestal, que provean productos de calidad para el mercado interno y externo, la dotación de infraestructura, la tecnificación y recuperación de suelos, la investigación científica y la transferencia de tecnología".

Bajo este mandato, la actual administración del MAG, plantea reorientar el sector agropecuario y rural hacia un modelo de desarrollo sostenible que conlleve a garantizar la competitividad, soberanía y seguridad alimentaria con identidad nacional, por ello es menester la incorporación de una nueva visión y roles que requieren un nuevo marco orientador que justifique, fundamente y oriente las iniciativas hacia la construcción de capacidades conceptuales, metodológicas y culturales para la gestión de la innovación institucional, hacia un esfuerzo de mejoramiento de prestación de servicios a los clientes externos del MAG.

Desde el compromiso con el sector agropecuario nacional y fundamentalmente con los pequeños y medianos productores, el MAG se propone desarrollar una gestión innovadora y transparente, desarrollar una gestión con características participativas y transparentes, con enfoque de equidad, que pretenda la sustentabilidad que estimule la competitividad, que promueva la descentralización y desburocratización, que fomente la interculturalidad, y que garantice la seguridad y soberanía alimentaria con identidad.

LA MISIÓN[4]

El Ministerio de Agricultura y Ganadería brinda servicios de calidad que responden a las necesidades de sus clientes, motiva y desarrolla su talento humano, comunica permanentemente, orienta, norma y capacita al sector agropecuario, agroindustrial, agroforestal y de riego.

[3] http://www.mag.gov.ec/docs
[4] http://www.mag.gov.ec/docs/elmag_70.htm

LA VISIÓN[5]

Un Ministerio de Agricultura y Ganadería, proactivo, motivado, honesto, moderno, eficiente y con recursos, que facilita los procesos de información, concertación y provisión de servicios de apoyo para el desarrollo sostenible de un sector Agropecuario, Agroindustrial, Agroforestal y de Riego, altamente competitivo, con enfoque humano, generando credibilidad, confianza y valor a sus clientes.

OBJETIVOS ESTRATÉGICOS[6]

- Elevar la Competitividad de los encadenamientos agroproductivos.
- Fortalecer las negociaciones internacionales de carácter agropecuario.
- Apoyar el Desarrollo Rural y Desarrollo Agropecuario, Agroforestal, Agroindustrial y Riego.
- Garantizar la Seguridad Alimentaria a través de elaboración de planes de contingencia.
- Fortalecer la Institución con énfasis en la descentralización, generación de tecnología, capacitación, fortalecimiento gremial, comunicación y lucha contra la corrupción.

POLÍTICAS[7]

- Política macroeconómica fiscal y comercial, orientada a la reactivación sostenible del sector agropecuario.
- Reactivación productiva a través del crédito, la generación y acompañamiento tecnológico y servicios de apoyo.
- Manejo sostenible de recursos naturales y ordenamiento territorial.
- Promoción de desarrollo sustentable de las comunidades campesinas afro-ecuatorianas, pueblos y nacionalidades indígenas, potenciando sus economías y sus capacidades de gestión territorial.
- Fortalecimiento de las organizaciones sociales, de productores e institucionalidad del sector

[5] http://www.mag.gov.ec/docs/elmag_71.htm
[6] http://www.mag.gov.ec/docs/elmag_72.htm
[7] http://www.mag.gov.ec/docs/elmag_73.htm

2.3.3 ESTRUCTURA ADMINISTRATIVA DEL MAG

El organigrama estructural del MAG con la Administración Central y las dependencias involucradas en este proyecto se puede ver en la figura 1.4.

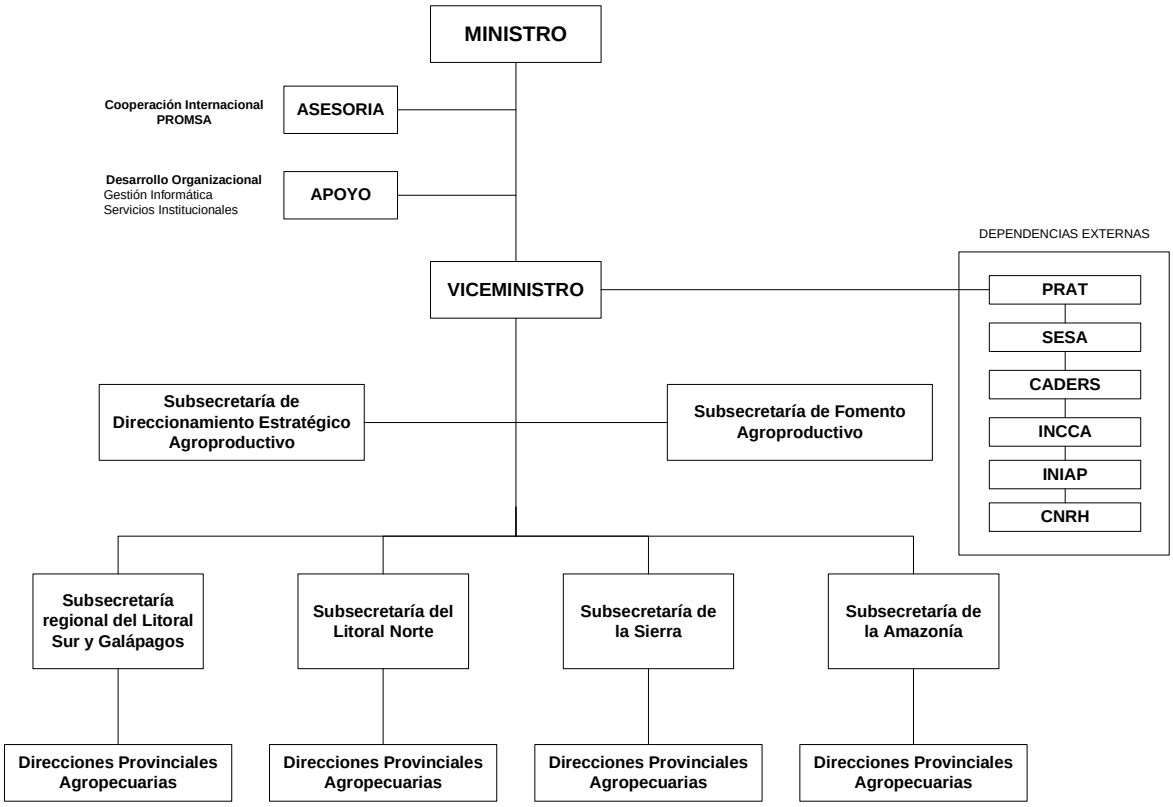


Fig. 1.4 Organigrama estructural del MAG

Partiendo de este organigrama, el Ministerio se puede dividir en dos grandes grupos, la administración central del MAG y las dependencias adscritas al MAG.

En la Administración Central del MAG, podemos encontrar el despacho del Ministro con sus asesores en auditoria, cooperación internacional, etc. y personal de apoyo como Desarrollo Organizacional con sus departamentos de Gestión Informática y Servicios Institucionales, y se encuentran ubicados en los pisos 12, 10 y planta baja, otro despacho que podemos encontrar y el mas importante del Ministerio es el del Viceministro con la Unidad Técnica de Gestión Estratégica para el sector agropecuario, y es el encargado de coordinar con las entidades adscritas y las Subsecretarías, este también se encuentra en el piso 10.

Bajo la dirección del Viceministro, se encuentran las Subsecretarías como la Subsecretaría de Direccionamiento Estratégico Agropecuario, que es la más grande del ministerio y que ocupa los pisos 5 y 6, otra Subsecretaría es la de Fomento Agropecuario y que se encuentra en el piso 11.

El MAG también consta con 4 Subsecretarías que no funcionan en el Edificio del Ministerio como la Subsecretaría Regional del Litoral Sur y Galápagos que se encuentra en la cuidad de Guayaquil, La Subsecretaría del Litoral Norte que se encuentra en la cuidad de Portoviejo, la Subsecretaría de la Sierra que se encuentra en la ciudad de Riobamba y la Subsecretaría de la Amazonía que se encuentra en la cuidad del Tena. Cada una de estas Subsecretarías tienen Direcciones Provinciales y que son una por cada cabecera provincial.

En cuanto a las dependencias adscritas al Ministerio tenemos: el PRAT (Programa de Regularización y Administración de Tierras Rurales), el SESA (Servicio Ecuatoriano de Sanidad Agropecuaria), el CADERS (Competitividad Agropecuaria y Desarrollo Rural Sostenible) que también se lo conoce como El Gran Japonés, el INCCA (Instituto Nacional de Capacitación Campesina), el INIAP (Instituto Nacional de Investigación Agropecuaria) y el CNRH (Consejo Nacional de Recursos Hídricos).

El presente proyecto se concentrará exclusivamente en la red del edificio matriz, que involucra la interconexión de la Administración Central del MAG con las dependencias mencionadas.

2.3.4 DESCRIPCIÓN DE LAS REDES DE DATOS

Luego de entender el organigrama del Ministerio e identificar los dos grupos a tratar, se realiza la descripción de las redes actuales del MAG y sus dependencias tanto en su tecnología como en su topología, se detallan los componentes de las redes: dispositivos de interconexión (Hub´s, Switchs, Routers), host´s (PC´s, servidores, Impresoras), software (sistemas operativos, aplicaciones), y se presentará los esquemas reales de interconexión tanto de componentes de la red así como la interconexión con Internet.

1.3.4.1 Tecnología y topologías de las redes del MAG y sus dependencias.

Por teoría se sabe que las redes LAN se pueden clasificar en redes de difusión y redes conmutadas. Analizando todas las redes del MAG y sus dependencias, se determina que son redes de difusión, ya que tienen un solo canal de comunicación compartido por todas las máquinas de la red. Los paquetes cortos que envía una máquina son recibidos por todas las demás. Un campo de dirección dentro del paquete especifica a quién se dirige. Al recibir el paquete, la máquina verifica el campo de dirección, si el paquete esta dirigido a ella, lo procesa, si esta dirigido a otra máquina lo ignora.

Las redes de difusión también ofrecen la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección. Cuando se transmite un paquete con este código, cada máquina en la red lo recibe y lo procesa, este modo de operación se llama difusión (broadcast[8]).

Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas, esto se conoce como multidifusión (multicast).

Estas redes de difusión se clasifican de acuerdo a la forma en que la información se difunde por el medio dando origen a las topologías lógicas de bus y de anillo, el MAG y sus dependencias poseen una topología lógica de bus. En esta topología, todos los elementos de la red están interconectados a través de un bus, este tipo de red funciona bajo la norma IEEE 802.3. Como el bus es compartido, se necesita verificar la disponibilidad del canal, para esto se utiliza el algoritmo Carrier Sense Multiple Access with Colition Detect (CSMA/CD) o acceso múltiple por censado de portadora y detección de colisión, cuya función se resume en los siguientes pasos:

- Escucha y define si alguna trama se recibe.
- Si no hay ninguna trama en el bus Ethernet, entonces transmite.
- Si hay alguna trama en el bus Ethernet, espera y luego escucha de nuevo.

[8] **Broadcast**, en castellano **difusión**, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea.

- Mientras está enviando, si una colisión ocurre, para, espera y escucha de nuevo.

Las redes Ethernet presentan diferentes especificaciones de capa 1, que no hacen más que indicar la velocidad, el tipo de señal a utilizar, el medio y la distancia máxima. 10Base2, 10/100BaseT, 1000BaseFX, etc. Por ejemplo 10Base2, significa que opera a una velocidad de 10Mbps, en banda base, por coaxial y a una distancia máxima de 200métros. 10BaseT, significa 10Mbps, en banda base, por par trenzado y hasta 100 metros.

Los desarrollos en hardware y equipos de concentración y switcheo, han llevado a las redes ethernet a convertirse en las redes LAN por excelencia. Su velocidad llega inclusive a Gigabit por segundo, en lo que se conoce como Gigabit Ethernet.

Desde el punto de vista físico, las redes del MAG y sus dependencias tienen una topología física en estrella.

A continuación, la tabla 1.1 resume las tecnologías y topología de las redes del MAG y sus dependencias.

		MAG	PRAT	SESA	CADERS	INCCA	INIAP	CNRH
Tecnología		IEEE 802.3	IEEE 802.3	IEEE 802.3	IEEE 802.3	IEEE 802.3	IEEE 802.3	IEEE 802.3
Topología	**Lógica**	Bus	Bus	Bus	Bus	Bus	Bus	Bus
	Física	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella	Estrella
Nivel Físico		10/100 BaseT	10/100 BaseT	10/100 BaseT	10/100 BaseT	10/100 BaseT	10/100 BaseT	10/100 BaseT

Tabla 1.1 Tecnología y topología de las redes del MAG y sus dependencias.

1.3.4.2 Sistema de cableado estructurado del MAG y sus dependencias.

La Administración Central del MAG y sus Dependencias actualmente constan de un cableado estructurado que cumple con las normas internacionales de categoría 5e, en su totalidad es implementada con elementos Alcatel y certificada con el nivel 3 de los estándares que consta de 10 tipos de pruebas que son: Longitud, Mapa de cableado, Insertion Loss (Atenuación), Near End Crosstalk (NEXT), Power Sun NEXT (PSNEXT), Atenuation Crosstalk Ratio (ACR), Power

Sun ACR (PSACR), Pérdida de retorno (Return Loss), Retardo de propagación (Propagation Delay), Delay Skew.

1.3.4.3 Equipamiento de las redes del MAG y sus dependencias.

Antes de mencionar el equipamiento de las redes involucradas en este proyecto, se detallarán los esquemas reales de estas redes para tener una idea clara de lo que vamos a interconectar.

Esquema de la red física de la Administración del MAG

La figura 1.5 muestra el esquema de la red física de la administración del MAG, se puede observar que se conforma de varias redes independientes que no se interconectan entre si, además la interconexión a Internet lo hacen a través de la red del CADERS.

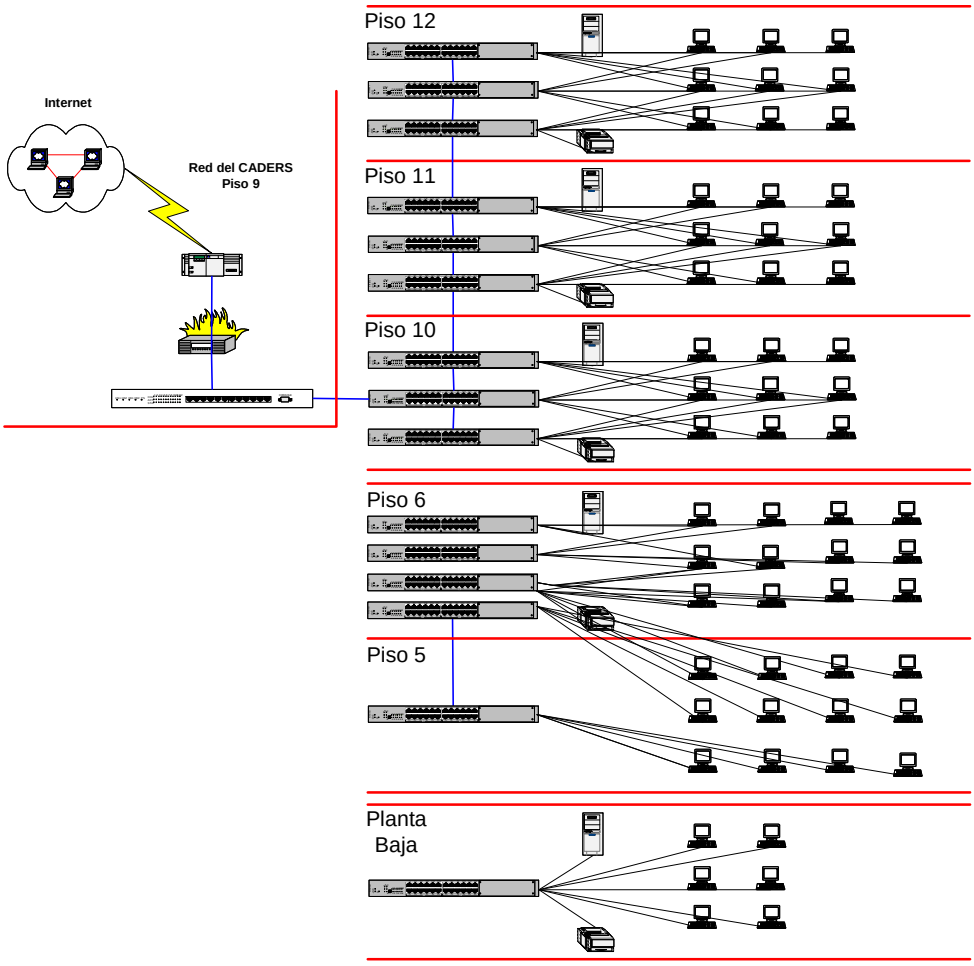


Fig. 1.5 Esquema de la red física de la Administración del MAG

Equipamiento de la red física de la Administración del MAG

A continuación se hace un inventario de equipos tanto de servidores, host, impresoras y de comunicación de la red de la Administración del MAG por pisos.

PISO 12

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	Archivos

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
19	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
17	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
14	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
15	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
1	HP	Laser Jet	Laser	X	
11	HP	Desk Jet	Inyección		X
9	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
2	3Com	3C16611	Hub	24	NO
1	3Com	3C16980	Switch	24	NO

Totales en el piso 12

Servidores	Host	Impresoras	Comunicaciones
1	65	21	3

PISO 11

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	A

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
18	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
14	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
17	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
13	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
1	HP	Laser Jet	Laser	X	
9	HP	Desk Jet	Inyección		X
8	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
2	3Com	3C16611	Hub	24	NO
1	3Com	3C16980	Switch	24	NO

Totales en el piso 11

Servidores	Host	Impresoras	Comunicaciones
1	62	18	3

PISO 10

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	A

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
23	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
21	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
11	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
9	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
1	HP	Laser Jet	Laser	X	
12	HP	Desk Jet	Inyección		X
8	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
2	3Com	3C16611	Hub	24	NO
1	3Com	3C16980	Switch	24	NO

Totales en el piso 10

Servidores	Host	Impresoras	Comunicaciones
1	64	21	3

PISO 6

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	A

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
29	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
21	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
5	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
11	Compaq	AP 550	P III	256MB	36.2GB	NTWst.
9	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
3	HP	Laser Jet	Laser	X	
13	HP	Desk Jet	Inyección		X
6	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
2	3Com	3C16611	Hub	24	NO
2	3Com	3C16980	Switch	24	NO

Totales en el piso 6

Servidores	Host	Impresoras	Comunicaciones
1	75	22	4

PISO 5

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	A

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
24	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
17	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
8	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
16	Compaq	AP 550	P III	256MB	36.2GB	NTWst.
8	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
2	HP	Laser Jet	Laser	X	
12	HP	Desk Jet	Inyección		X
4	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
2	3Com	3C16611	Hub	24	NO
2	3Com	3C16980	Switch	24	NO

Totales en el piso 5

Servidores	Host	Impresoras	Comunicaciones
1	73	18	4

PLANTA BAJA

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
5	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
9	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
1	HP	Desk Jet	Inyección		X
1	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
1	3Com	3C16980	Switch	24	NO

Totales en la planta baja

Servidores	Host	Impresoras	Comunicaciones
0	14	2	1

Totales en el MAG

Servidores	Host	Impresoras	Comunicaciones
5	353	102	18

Esquema de la red física del PRAT

La figura 1.6 muestra el esquema de la red física del PRAT, este se encuentra ubicado en el piso 10 y se localiza en el mismo rack del MAG y se conecta en cascada con un switch de este piso, la interconexión a Internet lo hacen a través del CADERS al igual que el MAG.

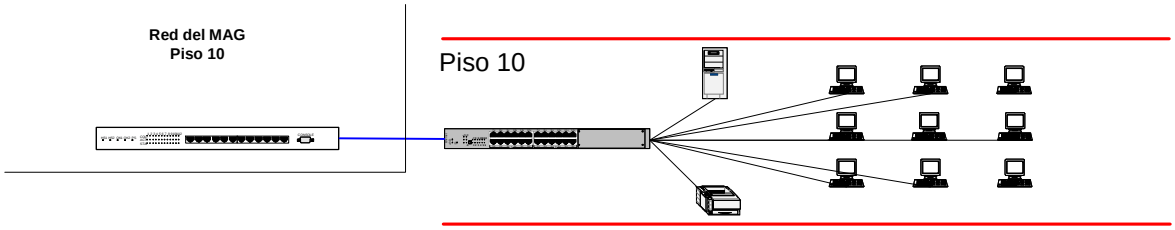


Fig. 1.6 Esquema de la red física del PRAT

Equipamiento de la red física del PRAT

A continuación se hace un inventario de equipos tanto de servidores, host, impresoras y de comunicación de la red del PRAT.

PRAT PISO 10

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	A

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
8	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
6	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
3	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
1	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
1	HP	Laser Jet	Laser	X	
1	HP	Desk Jet	Inyección		X
1	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
1	Cisco	2950	Switch	24	SI

Totales en el PRAT

Servidores	Host	Impresoras	Comunicaciones
1	18	3	1

Esquema de la red física del SESA

La figura 1.7 muestra el esquema de la red física del SESA, este se encuentra ubicado en el piso 9, la interconexión a Internet lo hacen a través del CADERS al igual que el MAG.

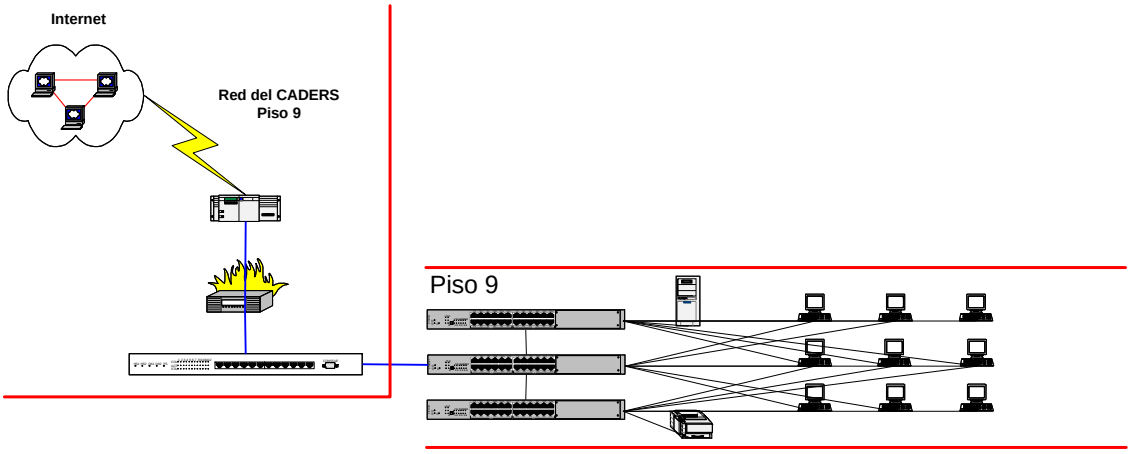


Fig. 1.7 Esquema de la red física del SESA

Equipamiento de la red física del SESA

A continuación se hace un inventario de equipos tanto de servidores, host, impresoras y de comunicación de la red del SESA.

SESA PISO 9

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	A

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
21	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
17	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
15	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
23	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
2	HP	Laser Jet	Laser	X	
3	HP	Desk Jet	Inyección		X
2	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
2	Cisco	2950	Switch	48	SI
1	3Com	3C16981A	Switch	24	NO

Totales en el SESA

Servidores	Host	Impresoras	Comunicaciones
1	76	7	3

Esquema de la red física del CADERS

La figura 1.8 muestra el esquema de la red física del CADERS, este se encuentra ubicado en el piso 9, y es el único departamento que tiene la salida a Internet bajo línea dedicada.

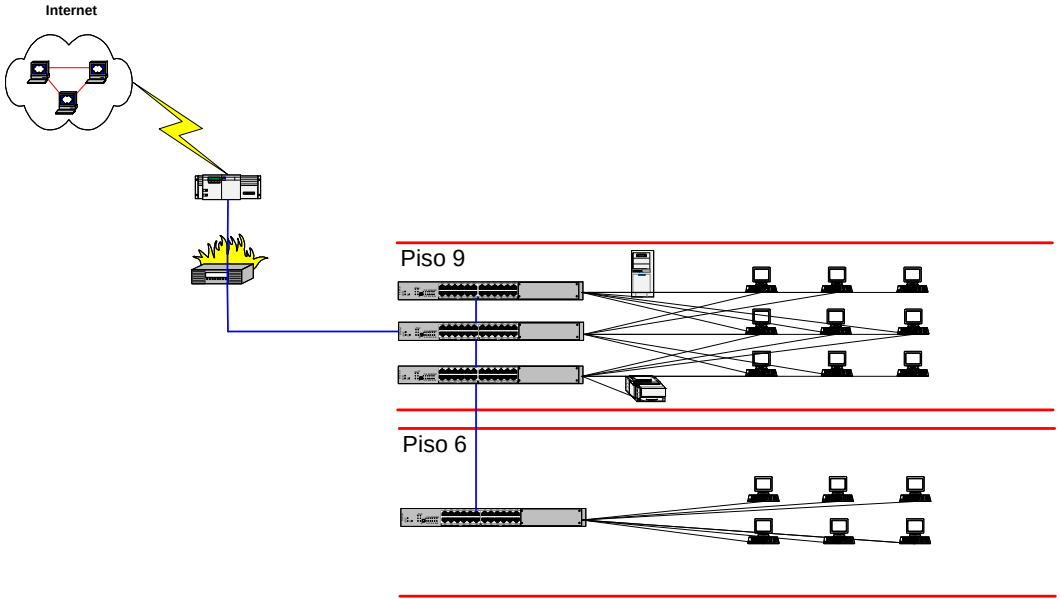


Fig. 1.8 Esquema de la red física del CADERS

Equipamiento de la red física del CADERS

A continuación se hace un inventario de equipos tanto de servidores, host, impresoras y de comunicación de la red del CADERS.

CADERS PISO 9

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	A

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
20	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
14	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
10	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
27	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
3	HP	Laser Jet	Laser	X	
5	HP	Desk Jet	Inyección		X
1	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
2	Cisco	2900	Switch	24	SI
1	Cisco	3500	Switch	24	SI

Totales en el CADERS

Servidores	Host	Impresoras	Comunicaciones
1	71	9	3

Esquema de la red física del INCCA

La figura 1.9 muestra el esquema de la red física del INCCA, este se encuentra ubicado en el piso 6, este departamento no tiene la salida a Internet.

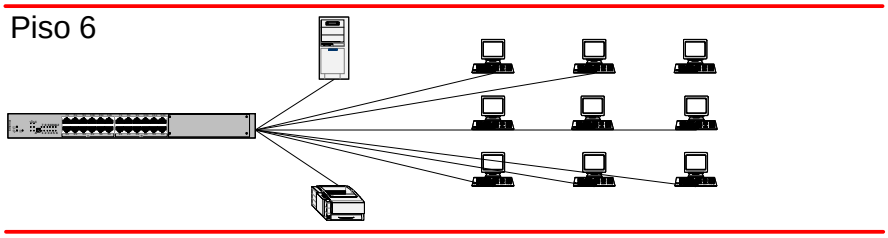


Fig. 1.9 Esquema de la red física del INCCA

Equipamiento de la red física del INCCA

A continuación se hace un inventario de equipos tanto de servidores, host, impresoras y de comunicación de la red del INCCA.

INCCA PISO 6

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	A

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
8	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
5	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
6	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
1	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
1	HP	Laser Jet	Laser	X	
1	HP	Desk Jet	Inyección		X
1	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
1	Cisco	2900	Switch	24	SI

Totales en el INCCA

Servidores	Host	Impresoras	Comunicaciones
1	20	3	1

Esquema de la red física del INIAP

La figura 1.10 muestra el esquema de la red física del INIAP, este se encuentra ubicado en el piso 4, este departamento no tiene la salida a Internet.

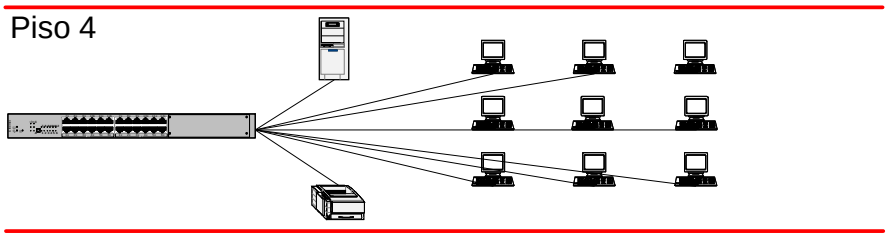


Fig. 1.10 Esquema de la red física del INIAP

Equipamiento de la red física del INIAP

A continuación se hace un inventario de equipos tanto de servidores, host, impresoras y de comunicación de la red del INIAP.

INIAP PISO 4

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	A

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
10	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
4	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
4	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98
1	Clones		P III	128MB	20GB	Win 2000

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
1	HP	Laser Jet	Laser	X	
1	HP	Desk Jet	Inyección		X
1	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
1	DLink	DES 1024R	Switch	24	SI

Totales en el INIAP

Servidores	Host	Impresoras	Comunicaciones
1	19	3	1

Esquema de la red física del CNRH

La figura 1.11 muestra el esquema de la red física del CNRH, este se encuentra ubicado en el piso 4, este departamento no tiene la salida a Internet.

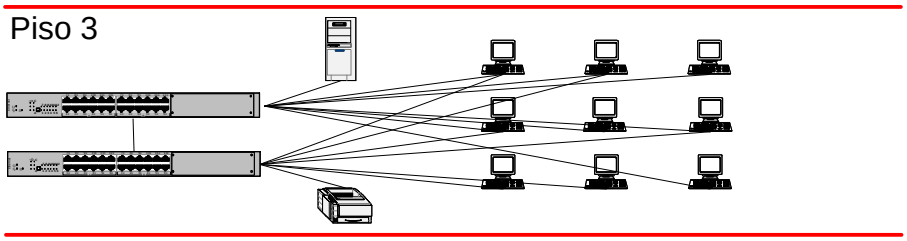


Fig. 1.11 Esquema de la red física del CNRH

Equipamiento de la red física del CNRH

A continuación se hace un inventario de equipos tanto de servidores, host, impresoras y de comunicación de la red del CNRH.

CNRH PISO 3

Servidores

Cant.	Marca	Modelo	Procesador	Mem.	Disco	S. O.	Tipo
1	Compaq	Proliant	P III	256MB	140GB	NT Serv	A

Host

Cant.	Marca	Modelo	Procesador	Memoria	Disco	S. O.
32	Compaq	Deskpro EP	P III	128MB	10GB	NT Wst.
23	Compaq	Deskpro EN	P III	128MB	10GB	NT Wst.
8	Compaq	Deskpro 2000	P I	32MB	3.2GB	Win 98

Impresoras

Cant.	Marca	Modelo	Tipo	De red	Local
1	HP	Laser Jet	Laser	X	
2	HP	Desk Jet	Inyección		X
2	Epson	FX 1170	Matricial		X

Dispositivos de interconexión

Cant.	Marca	Modelo	Tipo	Puertos	Administrable
2	Cisco	2900	Switch	24	SI

Totales en el CNRH

Servidores	Host	Impresoras	Comunicaciones
1	63	5	2

Luego de este análisis e inventario de las redes actuales del MAG y sus dependencias se puede determinar el número de puntos de datos que tenemos actualmente y se resume en la tabla 1.2.

NÚMERO DE PUNTOS DE RED EN TODO EL MINISTERIO					
		SERV	**HOST**	**IMP. RED**	**Total Puntos**
Adm, MAG	Piso 12	1	65	1	67
	Piso 11	1	62	1	64
	Piso 10	1	64	1	66
	Piso 9		21		21
	Piso 6	1	75	3	79
	Piso 5	1	73	2	76
	P B		14		14
	Total	**5**	**374**	**8**	**387**
PRAT	Piso 10	1	18	1	**20**
SESA	Piso 9	1	76	2	**79**
CADERS	Piso 9	1	71	3	75
	Piso 6		26		26
	Total	**1**	**97**	**3**	**101**
INCCA	Piso 6	1	20	1	**22**
INIAP	Piso 4	1	19	1	**21**
CNRH	Piso 3	1	63	1	**65**

Tabla 1.2 Número de puntos de red en todo el Ministerio.

1.3.4.4 Inventario de las aplicaciones existentes

La Administración Central del MAG y las Dependencias utilizan la plataforma Intel-Microsoft básicamente para correr las aplicaciones comúnmente usadas como control de usuario, correo electrónico, navegador Web, etc. Además utilizan la típica aplicación Office para las tareas de oficina.

A parte de estas aplicaciones, existen otras aplicaciones creadas específicamente para la Administración Central y las Dependencias, las cuales detallamos a continuación.

Aplicación: Centro de Atención de Usuarios - CAU

Objetivo de la aplicación: Soporte HelpDesk para recepción y solución de consultas informáticas, desarrollado para entorno web.

Descripción: Partiendo del operador que toma nota de una consulta informática, genera el parte correspondiente, asignándole, si no puede resolverlo él en primera instancia, el grupo de trabajo. Los integrantes de dicho grupo, asignan el parte a uno de los técnicos para su resolución. Durante la vida del parte este

puede traspasarse a otros técnicos o a otro grupo de trabajo distintos al inicial, hasta que queda marcado como solucionado.

Dependencia: Administración Central del MAG
Sistema Operativo: La aplicación esta desarrollada para utilizarse a través de navegador.
Base de Datos: Servidor DOMINO v. 5.0.10. En este caso corriendo sobre solaris, pero por la naturaleza del domino es independiente del SO del servidor.
Lenguaje de Programación: Lotus Notes v. 5.0.10.

Aplicación: Gestión de Almacén

Objetivo de la aplicación: Gestión de los procesos que conlleva el control del funcionamiento del Almacén General del SESA.

Descripción: La aplicación contempla 3 tipos de usuarios: peticionarios, gestores y administrador central. A nivel de usuario peticionario controla los procesos relacionados con la gestión de las solicitudes de petición y devolución de material y les permite consultar su consumo, así mismo, tienen acceso a un catálogo de artículos (incluye foto) personalizado según perfil.

A nivel de gestor - administrador de almacén controla: los usuarios, la creación de concurso, la generación de expedientes, el trámite de las peticiones y devoluciones, los pedidos a proveedor, el control de albaranes y facturas de proveedores, control de stock, estadísticas de consumo, creación y envío de noticias, traspasos a históricos, generación de fichero de gastos, etc.

Dependencia: SESA
Sistema Operativo: Windows 9X o superior
Base de Datos: Oracle 8i
Lenguaje de Programación: Power Builder 6.5

Aplicación: Gestión de Correos

Objeto de la aplicación: Gestionar el servicio integral de correos y mensajería.

Descripción: Hay que gestionar y controlar tanto los envíos que realizan, la procedencia, y la facturación de los distintos servicios, según el tipo de servicio hay que tener en cuenta el iva o algún tipo de bonificación a aplicar. Realiza traspasos a históricos y generación de informes y fichero de gastos.

Dependencia: SESA, INCCA
Sistema Operativo: Windows 9X o superior
Base de Datos: Oracle 8i
Lenguaje de Programación: Power Builder 8.0.3

Aplicación: Gestión y Control de Fotocopias

Objeto de la aplicación: Gestiona y calcula costes de fotocopias y trabajos realizados en cartografía.

Descripción: A partir de diferentes fotocopiadoras o máquinas con las que se pueden elaborar trabajos de cartografía, encuardenación etc. se pueden almacenar los trabajos realizados y hacer facturaciones por los servicios prestados mensualmente a partir de las diferentes tarifas anuales.

También se calculan y se distribuyen los costos de los trabajos por Departamentos, Direcciones Generales o Centros de trabajo. Se elaboran Informes y Ficheros para enviar a los Departamentos, conociendo igualmente la evolución de los costos por máquinas, años, meses etc.

Dependencia: CNRH
Sistema Operativo: W98 ó superior
Base de Datos: Oracle 8i
Lenguaje de Programación: Power Builder 6.5

Aplicación: CIAAP

Objeto de la aplicación: Su función es gestionar los cursos de formación dirigidos al campesinado, y cuya administración son competencia del INCCA.

Descripción: Alta del curso, con el temario, aula, horario, convocatoria, materia y profesorado. Publicación del curso en el Boletín Oficial y en el portal del INCCA.

Recepción de instancias por vía Web y por papel. Generación de cartas de admisión y no admisión, cambios en la convocatoria, etiquetas, hojas de firmas de asistencia, encuestas, y diplomas. Envío de las notificaciones por E-mail de la admisión y no admisión, y de los cambios de la convocatoria. Generación del pago del profesorado para su comunicación a contabilidad.

Dependencia: INCCA
Sistema Operativo: Windows 98/2000/XP
Base de Datos: Oracle 8i
Lenguaje de Programación: PowerBuilder 8.0.3 para la parte C/S y JSP-Oracle Portal para la parte Web.

Aplicación: RegESAccess

Objeto de la aplicación: La aplicación sirve para llevar un registro interno de los diferentes documentos a los que se dan entrada y salida desde el PRAT.

Descripción: La aplicación está basada en una pantalla de menú a partir de la que se accede a los documentos de entrada, los de salida o temas. Los temas son agrupaciones de documentos de entrada y salida. En cada apartado está la opción de agregar nuevos documentos, revisarlos todos o seleccionar un conjunto para realizar alguna tarea de revisión, edición o impresión.

Dependencia: PRAT
Sistema Operativo: Windows 95-98
Base de Datos: Microsoft Access 97
Lenguaje de Programación: Visual Basic para Aplicaciones

Aplicación: Reserva de salas

Objeto de la aplicación: Reserva y consulta de reservas de salas de reuniones.

Descripción: Aplicación para la reserva y consulta de reservas de salas de reuniones, consulta por navegador.

Dependencia: INCCA
Sistema Operativo: Acceso por navegador

Base de Datos: Microsoft Access 97
Lenguaje de Programación: Visual Basic para Aplicaciones

2.4 REQUERIMIENTOS DE LA RED DEL MAG.

Tanto las dependencias como la Administración Central del MAG tienen los mismos requerimientos de red, por lo que se tratarán de forma conjunta en este capítulo. Para tener un mejor entendimiento de los requerimientos de la red del MAG, vamos a dividir a estos en requerimientos de tráfico de la red y requerimientos de seguridad en la red.

2.4.2 REQUERIMIENTOS DE TRÁFICO DE LA RED

El análisis del tráfico de red en términos de volumen es muy utilizado para determinar capacidades y rendimientos.

Con el fin de dimensionar la capacidad de los enlaces se debería realiza un análisis de las necesidades de tráfico entre las Dependencias y la Administración Central del MAG en horas pico, pero por no existir esta conexión y no existir un referencial anterior, los distintos tráficos se pueden suponer que están en el orden de Mbps, y como los estándares son 10, 100, 1000 Mbps. se escogen los más altos.

Se realizó un análisis del tráfico de datos que circula por las redes independientes de la Administración Central del MAG y de las Dependencias y se asumió este como el máximo tráfico que circulará por los Backbones de la red a construir, los mismos que son los siguientes.

Tráfico de la administración del MAG

Mediante el uso de un software de monitoreo de tráfico llamado *Ethereal* versión 0.99.0 que es de uso libre, se determinó el volumen de tráfico entrante y saliente que circula a través de la red de la Administración del MAG en los pisos 5 y 6.

El software fue instalado en un computador de la red de la Administración del MAG y se tomaron medias diarias en horas pico (de 10h00 a 12h00 según información suministrada por el personal administrador de la red); sacando como

referencia para calcular el tráfico que circula en la red de la administración del MAG el correspondiente al día de tráfico circulante más alto, cuyos resultados se muestran en las figuras 1.12 y 1.13.

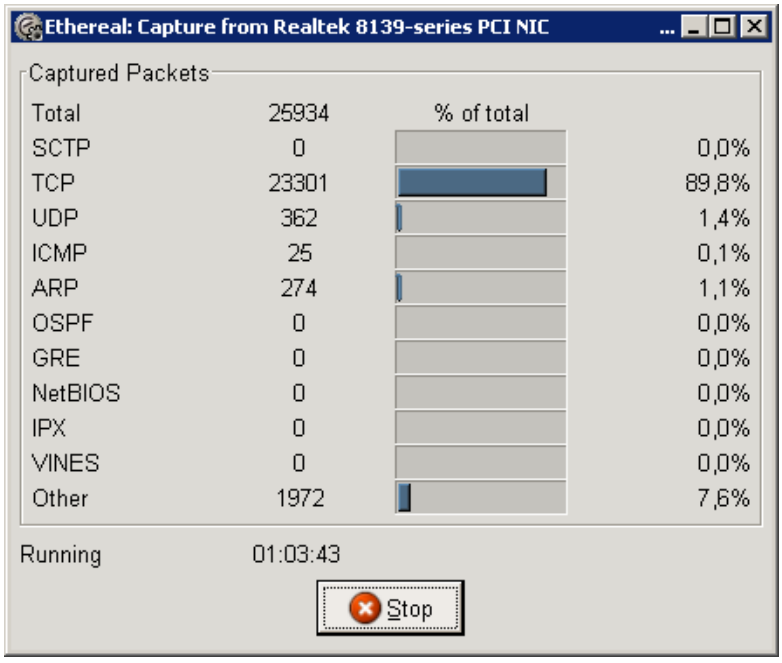


Figura 1.12 Tráfico medido en la Administración Central del MAG

Para la estimación del ancho de banda utilizado por una computadora, se tomó el número total de paquetes capturados por esta en 1 hora, 3 minutos y 43 segundos y que corresponden a 25.934 paquetes.

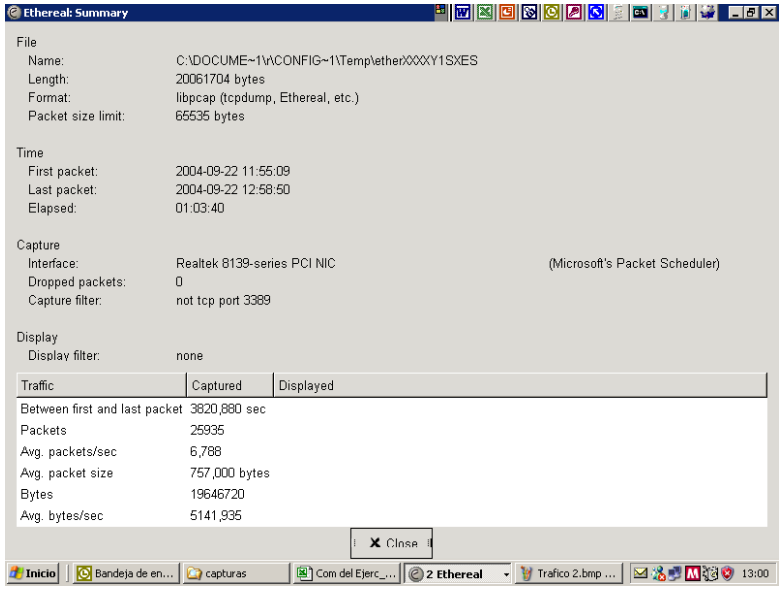


Figura 1.13 Resumen del tráfico medido en la Administración Central del MAG

El tamaño máximo de un paquete ethernet es de 1.518 bytes incluyendo cabecera y trailer. Se tomó las estadísticas que suministra el software para determinar el tamaño promedio de los paquetes capturados como se muestra en la figura 1.13, y que resultó ser de 757bytes.

$$Capacidad = \frac{25.934\ [tramas]}{63*60+43[segundos]} \times \frac{757[bytes]}{1[trama]} \times \frac{8[bits]}{1[byte]} \times \frac{1[Kb]}{1000[bits]} = 41{,}082[Kbps]$$

El tráfico total se lo calcula multiplicando la capacidad por el número de computadoras conectadas a la red y por un porcentaje de acceso simultáneo que es del 30% (información suministrada por el personal administrador de la red y centros de computo), es decir que del total de computadoras, el 30% se encuentran usando simultáneamente los servicios de la red.

*Tráfico Total = Capacidad * # total de computadoras * porcentaje de acceso simultáneo*
Tráfico Total = 41,082[Kbps] * 155 * 0.3*
Tráfico Total = 1.910,31 [Kbps]

La red que dispone al momento la Administración del MAG en los pisos 5 y 6 es de 100Mbps por lo que satisface el tráfico interno que por ella circula.

Si se supone que todo este tráfico circulará por el Backbone y que este será de 1Gbps, entonces satisfacerá al tráfico que circularía por él.

Trafico en el CNRH

De igual manera que en la Administración del MAG, se instaló el software *Ethereal* en una computadora de la red del CNRH. Se realizó el monitoreo tomando las mismas consideraciones del caso anterior, obteniendo como resultado los datos que se muestran en la figura 1.14.

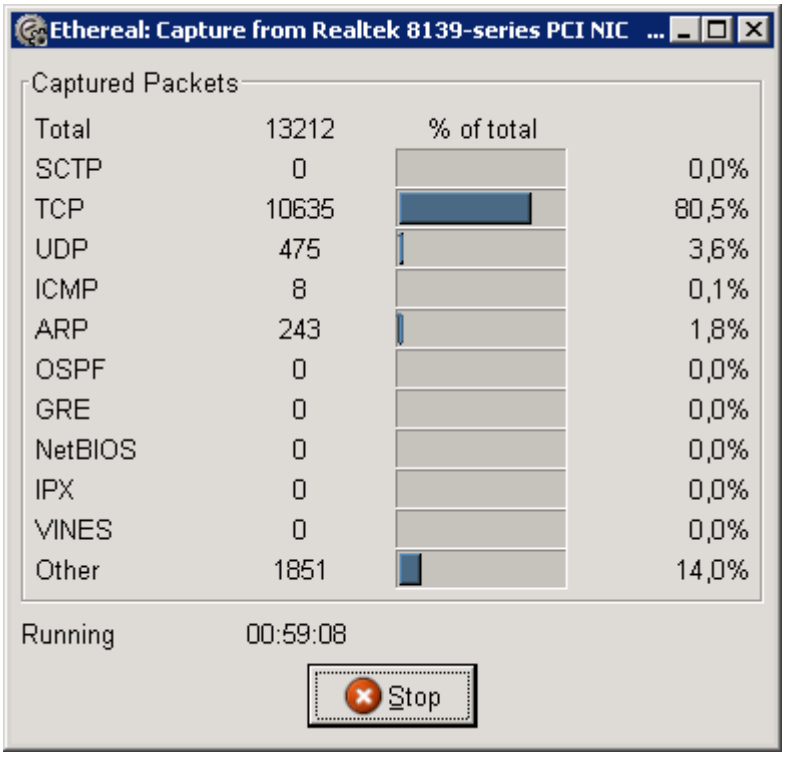


Figura 1.14 Tráfico medido en el CNRH

El total de paquetes capturados en el tiempo de 59 minutos y 8 segundo fue de 13.212, se mantuvo el 30% de acceso simultáneo y el tamaño de paquete de 757 bytes.

$$Capacidad = \frac{13212\ [tramas]}{59*60+8[segundos]} \times \frac{757[bytes]}{1[trama]} \times \frac{8[bits]}{1[byte]} \times \frac{1[Kb]}{1000[bits]} = 22.551\ [Kbps]$$

*Tráfico Total = Capacidad * # total de computadoras * porcentaje de acceso simultáneo*
Tráfico Total = 22.551 [*Kbps*] * 65 * 0.3
Tráfico Total = 439,75 [Kbps]

Para el resto de redes se procedió de la misma manera para encontrar el tráfico total y se determinaron los siguientes valores como se detalla en la tabla 1.3.

		Total Puntos	Tráfico de Datos [Kbps]
Adm, MAG	Piso 12	67	2.341,12
	Piso 11	64	
	Piso 10	66	
	Piso 9	21	
	Piso 6	79	1.910,31
	Piso 5	76	
	PB	14	44,64
PRAT	Piso 10	20	1.214,82
SESA	Piso 9	79	1.023,49
CADERS	Piso 9	75	1.142,18
	Piso 6	26	
INCCA	Piso 6	22	75,02
INIAP	Piso 4	21	87,99
CNRH	Piso 3	65	439,75
TOTAL		**695**	**8.279,32**

Tabla 1.3 Tráfico de datos en todas las redes del Ministerio.

2.4.3 REQUERIMIENTOS DE SEGURIDAD EN LA RED

No hay ninguna duda que hoy en día, la seguridad informática es tan importante como la seguridad tradicional de una empresa. Por ello el MAG y sus dependencias necesitan de soluciones para todas las posibles amenazas, intrusos, virus y ataques tanto externos como internos.

Se requiere también establecer políticas de seguridad entre la Administración Central del MAG y las dependencias para que la información sea privada y confidencial.

Seguridad Física

Este punto se refiere principalmente a la seguridad que debe tener el sitio donde se alojen los equipos principales de la red. Este cuarto donde se concentrará el cableado y los servidores debe cumplir con todas las características de seguridad, accesibilidad, facilidad de administración y facilidad de cableado.

Seguridad Departamental

Esta seguridad se refiere a la independencia que deben tener las redes de las dependencias y la Administración Central, que la información confidencial de una

dependencia no sea manipulada por otra excepto la información que se debe compartir. Para lograr esto, las redes deberán interconectarse mediante dispositivos de encaminamiento, para que todas las conexiones que se establezcas se realicen a través de ellos, mientras son examinadas y evaluadas.

Seguridad Perimetral

Esta seguridad se refiere a la protección que deben tener la red del MAG de accesos externos no autorizados. Como la idea es que todas las dependencias tengan su salida al Internet a través del MAG, esta seguridad dependerá exclusivamente del MAG para lo cual será necesario que se instale un equipo para la conexión con el exterior y que proporcione seguridad a toda la red, particularmente en lo que se refiere al acceso a Internet, que representa la amenaza mas importante a la seguridad del Ministerio.

Protección Corporativa por software

Se refiere a programas que permiten proteger a la red de otros programas maliciosos, para lo cual se instalará un sistema de protección corporativo por software, que proteja de virus, spam, spyware, troyans, ataques de intrusos a los servidores y las estaciones, que maneje estadísticas y reportes y que tenga una administración centralizada.

2.4.4 SERVICIOS DE RED REQUERIDOS

No hay duda que hoy en día los servicios que ofrecen las redes informáticas han pasado a ser indispensables para una institución. Ya no solo se necesita una conexión a Internet sino también servicios de Intranet.

Tomando como referencia otras instituciones gubernamentales, el MAG tendrá varios servicios de red, a estos servicios se los puede dividir en servicios de Internet, servicios de Intranet y servicio de acceso remoto.

1.4.4.1 Servicios de Internet

Servicio Web y navegación

Miles de personas usan Internet asiduamente para encontrar los servicios y productos que necesitan. El MAG desea establecer su sitio Web y controlar los

parámetros de su propio servidor. La dirección del Servidor Web del MAG sería http://www.mag.gov.ec, en él podremos encontrar información general sobre los servicios que presta, sitios agropecuarios, sitios gubernamentales, organismos internacionales, etc. además de los enlaces con los sitios Web de las distintas dependencias.

Servicio de nombres de dominio(DNS)

El MAG quiere gestionar su propio servidor de nombres, desea implementar un servidor local de DNS. Los servidores locales no tienen autoridad sobre ningún dominio, se limitan a contactar con otros servidores para resolver las peticiones de los clientes DNS. Estos servidores mantienen una memoria caché con las últimas preguntas contestadas. Cada vez que un cliente DNS le formula una pregunta, primero consulta en su memoria caché. Si encuentra la dirección IP solicitada, se la devuelve al cliente; si no, consulta a otros servidores, apunta la respuesta en su memoria caché y le comunica la respuesta al cliente.

Servicio de Correo Electrónico

El e-mail o correo electrónico se utiliza para la transferencia de información (tanto textos simples como elementos multimedia) que no necesita comunicación en tiempo real, esto es, el receptor y el emisor no tienen que estar necesariamente accediendo al servicio al mismo tiempo para enviar y recibir la información. Es un sistema de almacenamiento y reenvío, siendo la comunicación no interactiva.

El MAG desea instalar su propio servidor de correo para controlar su propio tráfico, el correo electrónico se encontrará asociado a la cuenta de que dispone cada miembro del MAG, el formato de la dirección de correo sería nombre_usuario@mag.gov.ec.

Será responsabilidad del usuario asegurarse que el buzón no llegue a saturarse. Para ello deberá de realizar una limpieza periódica del mismo eliminando mensajes antiguos. Si se supera la capacidad máxima, el servidor rechazará todos los correos hacia el usuario.

Servicio de VPN (Virtual Private Network)

Esta tecnología le permitirá al MAG conectarse con instituciones gubernamentales mediante Internet. Podrán conectarse a la red interna desde el SRI, CAE, Banco Central, BNF, etc., de forma segura mediante conexiones cifradas, de manera transparente.

1.4.4.2 Servicios de Intranet

El MAG le ofrecerá varios servicios para crear una Intranet rica en contenidos y de utilidad para su gestión. La infraestructura informática ha evolucionado y los servicios internos ya son indispensables para el funcionamiento mas eficaz dentro de las empresas, así tenemos:

Servicio de autenticación.

Todos los usuarios del MAG para el control de acceso debe identificarse conectándose con un servidor de dominio, en el cual se autentificarán por medio de un nombre de usuario y una clave de acceso. Si ambos son correctos, el usuario puede conectarse a la red.

Servicio de archivos compartidos

Luego del análisis y estudio de los sistemas internos del ministerio se desprende la necesidad de compartir archivos entre dependencias o empleados, o simplemente se desea mantener los archivos importantes en un lugar centralizado donde sea simple acceder y fácil hacer copias de seguridad.

Servicio de impresión.

El MAG tendrá compartidas impresoras de alta calidad, capacidad y costo entre múltiples usuarios y dependencias, reduciendo así el gasto. Existirá un equipo servidor con capacidad de almacenamiento propio donde se almacenarán los trabajos en espera de impresión.

Una variedad del servicio de impresión es la disponibilidad de servidores de fax, los cuales ponen al servicio de la red sistemas de fax para que se puedan enviar éstos desde cualquier estación. En ciertos casos, es incluso posible enviar los

faxes recibidos por correo electrónico al destinatario. Este servicio se está pensando instalar en un futuro en todo el Ministerio.

Servicio de DHCP

Debido a la gran cantidad de equipos a instalarse en todo el ministerio se ve en la necesidad de instalar un servidor de DHCP el cual nos permita asignar direcciones IP automáticas a las estaciones y solo dejar direcciones fijas a los servidores y otros equipos que así lo requieran.

1.4.4.3 Servicio de Acceso Remoto (RAS)

Es un servicio que se implantará en un futuro, el MAG dispondrá de un servidor de acceso remoto con módems a 56 Kbps. El protocolo de acceso utilizado será PPP tipo PAP. El teléfono del servidor de acceso remoto esta por definirse. El costo de la llamada telefónica necesaria para poder conectarse a la red corre por cuenta del usuario, siendo este el único gasto por parte de éste.

2.5 PROYECCIONES Y PERSPECTIVAS

Como se describió en este capítulo en la estructura administrativa del MAG, la Administración Central tiene cuatro subsecretarías que administran el agro en las distintas regiones de nuestro país y estas son la Subsecretaría Regional del Litoral Sur y Galápagos, la Subsecretaria del Litoral Norte, la Subsecretaria de la Sierra y la Subsecretaría de la Amazonía que están dirigidas desde las Direcciones Provinciales ubicadas en las ciudades de Guayaquil, Portoviejo, Riobamba y Tena respectivamente.

Estas Subsecretarías Regionales a su vez gobiernan las 22 provincias del país por medio de sus Direcciones Provinciales ubicadas en las cabeceras provinciales que son las capitales de cada provincia como se detalla a continuación en la tabla 1.4:

Litoral Norte	Litoral Sur	Sierra	Amazonía
Esmeraldas	Guayas	Carchi	Sucumbíos
Manabí	Los Ríos	Imbabura	Fco. de Orellana
	El Oro	Pichincha	Napo
	Galápagos	Cotopaxi	Pastaza
		Tungurahua	Morona Santiago
		Chimborazo	Zamora Chinchipe
		Bolívar	
		Cañar	
		Azuay	
		Loja	

Tabla 1.4 Subsecretarías y sus Direcciones Provinciales

Actualmente estas Direcciones Provinciales a excepción de las Subsecretarías, cuentan con una pequeña red LAN con cableado categoría 5e y un grupo de trabajo, tienen estaciones Compaq Deskpro 2000 y un equipo Workstation AP400 igual Compaq, no cuentan con conexión a Internet ni ningún sistema de telecomunicación para comunicarse con la Administración Central.

Las Subsecretarías cuentan con una red LAN más grande igual con cableado categoría 5e pero ya disponen de un dominio, tienen equipos Compaq Deskpro 2000 y un servidor Compaq Proliant 2500, tienen un acceso vía Dial-up para conectarse a Internet .

A continuación presentamos la tabla 1.5 resumiendo la cantidad de equipos existentes en cada una de las Direcciones Provinciales, cabe señalar que el SIGEF y el SIGAGRO son divisiones administrativas dentro de las Direcciones Provinciales.

PROVINCIAS	ESTACIONES		SERVIDORES y WORKSTATION	IMPRESORAS		
	SIGEF	SIGAGRO		MATRICIALES	LASER	INYECCION
AZUAY	4	1	1	1	1	1
BOLIVAR	4	1	1	1	1	1
CAÑAR	3	1		1	1	1
CARCHI	3	1		1	1	1
CHIMBORAZO	11	1	1	2	3	1
COTOPAXI	3	1		1	1	1
EL ORO	4	1	1	1	1	1
ESMERALDAS	4	1	1	1	1	1
GALAPAGOS	3	1		1	1	1
GUAYAS	11	1	1	2	3	1
IMBABURA	4	1	1	1	1	1
LOJA	4	1	1	1	1	1
LOS RIOS	4	1	1	1	1	1
MANABI	11	1	1	2	3	1
MORONA	3	1		1	1	1
NAPO	3	1		1	1	1
ORELLANA	3	1		1	1	1
PASTAZA	3	1		1	1	1
PICHINCHA	43	22	5	1	24	20
SUCUMBIOS	3	1		1	1	1
TUNGURAHUA	8	1	1	1	1	1
ZAMORA	3	1		1	1	1
TOTALES	**142**	**43**	**16**	**25**	**51**	**41**

Tabla 1.5 Cantidad de equipos en las Direcciones Provinciales

El plan de Desarrollo Agrario y Rural para los siguientes periodos, presenta entre los objetivos estratégicos, una reforma institucional profunda, moderna y eficiente, con ajustes de recursos, costos y productividad de desempeño proponiéndose algunas actividades por objetivos y metas como:

Políticas de estado en donde consta Implementar un sistema informático para administrar datos veraces, reforma institucional presentando la propuesta de la nueva carta orgánica del MAG implementando el plan de selección, capacitación, promoción y distribución del personal, aumento de la producción agropecuaria de exportación y seguridad alimentaria, reordenamiento territorial y mejora de la propiedad de la tierra, condiciones y mecanismos de comercialización, reducción de la pobreza y la desigualdad entre otras.

Para lograr estos objetivos el MAG se propone implementar un sistema de información geográfica agraria el cual consiste en intercambiar información de suelos, climas, organizaciones campesinas, etc. en tiempo real y desde la fuente misma de la información.

Además se propone desarrollar un sistema de precios de productos agrícolas para transmitirlos a la Administración Central en tiempo real y desde los lugares en donde se obtengan los precios.

Se pretende comunicar a todas las Direcciones Provinciales mediante un sistema de telefonía IP.

Así mismo se propone implementar una biblioteca virtual relacionada al agro para fortalecer la capacitación propuesta y poder también tener una educación virtual o a distancia.

Como parte integral de este sistema informático se incluye la interconexión entre la Administración Central del MAG con las Subsecretarías Regionales y con las Direcciones Provinciales para poder intercambiar la información planteada anteriormente, las alternativas de tecnologías para la implementación de esta infraestructura WAN se la detalla en el capitulo 2.

CAPITULO 2

DISEÑO DE LA RED DE CAMPUS EN TRES CAPAS DEL MAG.

2.1 DISEÑO DE LA RED DE CAMPUS EN TRES CAPAS

2.1.1 INTRODUCCIÓN

Una red LAN es una red de comunicación entre computadoras que permite compartir información, en distancias relativamente cortas y a altas velocidades.

Implementar una red LAN, implica tener en cuenta varios aspectos claves. Uno es la elección del medio de transmisión, el cual pueden ser par trenzado, coaxial, fibra óptica o medios inalámbricos.

Otro es el método que se utilice para el control de acceso al medio. Los esquemas mas utilizados en LAN son CSMA/CD en IEEE802.3 y Token Passing en IEEE802.5 para el caso de las redes alámbricas.

El control de acceso al medio define la topología lógica de la red, siendo las más conocidas el anillo y el bus.

De esta manera podemos decir que los aspectos tecnológicos principales que determinan las características de una red LAN son:

- Topología física
- Topología lógica
- Técnica de control de acceso al medio
- Medio de transmisión

A continuación en la tabla 2.1 se describen los aspectos principales de una red LAN.

Tecnología	Medio	Método de acceso	Topología física	Topología lógica
802.3	Par trenzado	CSMA/CD	Estrella	Bus
802.5	Coaxial/par trenzado	Toke Passing	Estrella	Anillo

Tabla 2.1 Aspectos de una red LAN

A continuación se describe en términos generales la tecnología IEEE802.3 que es la que se usará en el presente proyecto.

2.1.2 LA TECNOLOGÍA IEEE 802.3

La versión original en banda base de esta técnica fue desarrollada por Xerox para redes LAN Ethernet, este desarrollo fue la base para la posterior especificación del estándar IEEE 802.3.

El estándar IEEE 802.3 presenta la siguiente arquitectura:

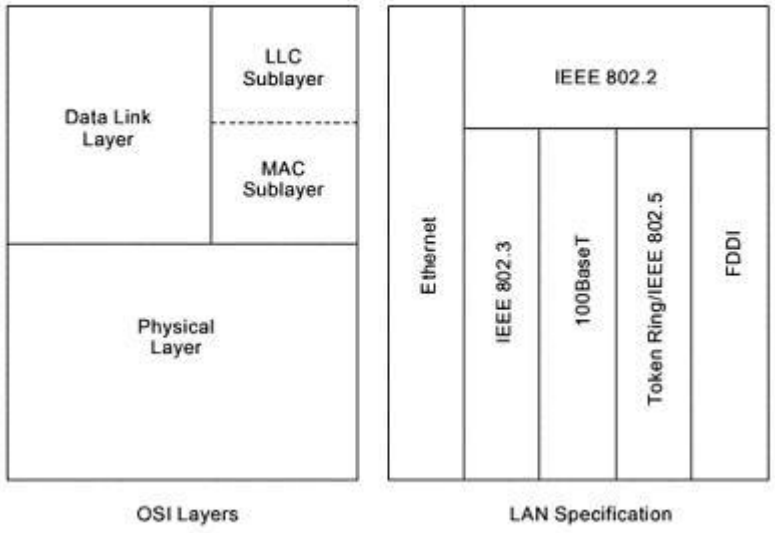


Fig. 2.1 Protocolos LAN y Modelo de Referencia OSI[9]

En la figura 2.1 se muestra la arquitectura de esta especificación y donde se puede observar la diferencia que existe entre la tecnología Ethernet e IEEE 802.3.

3.1.3 OBJETIVOS PARA EL DISEÑO DE LA RED

El primer paso en el diseño de la LAN del Ministerio es establecer y documentar los objetivos de diseño. Estos objetivos son específicos para cada organización o situación. A continuación se describen los objetivos para el diseño de la red de todo el MAG.

- Funcionalidad: La red debe suministrar conectividad de usuario a usuario y de usuario a aplicación con una velocidad y confiabilidad razonables.

[9] Cisco CCNA-CNAP Capitulo12: Protocolos LAN

- Escalabilidad: La red debe poder aumentar de tamaño. Es decir, la red original puede aumentar de tamaño sin que se produzcan cambios importantes en el diseño.
- Adaptabilidad: La red debe diseñarse teniendo en cuenta otras tecnologías que brinden valor agregado como voz sobre IP, seguridad, acceso, etc. La red no debería incluir elementos que limiten la implementación de nuevas tecnologías a medida que éstas van apareciendo.
- Facilidad de administración: La red debe estar diseñada para facilitar su monitoreo y administración, con el objeto de asegurar una estabilidad de funcionamiento constante.

3.1.4 CONSIDERACIONES PARA EL DISEÑO DE UNA RED

Para el diseño de una red con cualquier metodología que se use, es necesario tomar en cuenta las siguientes consideraciones:

- Función y ubicación de los servidores.
- Los dominios de colisión.
- La segmentación.
- Los dominios de broadcast.

2.1.4.1 Función y ubicación de servidores

Los servidores permiten que los usuarios de red se comuniquen y compartan archivos, impresoras y servicios. Los servidores ejecutan sistemas operativos especializados como por ejemplo NetWare, Windows, UNIX y Linux. Cada servidor por lo general está dedicado a una función, por ejemplo, correo electrónico, servidor de base de datos, etc.

Los servidores se pueden categorizar en servidores empresariales y servidores de grupo. Un servidor empresarial soporta todos los usuarios en la red ofreciendo servicios tales como Servidor de Dominio, Correo Electrónico o Sistema de Nombres de Dominio (DNS). El dominio, el correo electrónico o el DNS son servicios que cualquier host de una red necesita. En cambio un servidor de grupo soporta un conjunto específico de usuarios y servicios como por ejemplo el servidor de Desarrollo del CADERS.

El MAG contará con estos dos tipos de servidores, los servidores empresariales se encontrarán en un cuarto principal y los servidores de grupo en cada una de las dependencias de ser el caso.

2.1.4.2 Dominios de colisión

El segmento dentro de la red donde los paquetes se originan y colisionan se denomina Dominio de Colisión.

Las colisiones se producen en el medio compartido. Y se presentan cuando hay muchos ordenadores conectados a la red.

Las colisiones se producen por el método que utilizan los hosts para acceder al medio que en el caso de las redes IEEE 802.3 es el CSMA/CD.

Una dirección MAC, es una dirección de 48 bits, representados en hexadecimal. Los 48 bits están agrupados de 4 en 4, y hasta 12 dígitos, de los cuales los 6 primeros corresponden al fabricante o proveedor, y los 6 dígitos restantes al número de serie de la NIC (Network Interface Card).

En el método CSMA/CD, cada nodo debe disputar con otros nodos para acceder al medio compartido o al dominio de colisión. Si dos nodos transmiten al mismo tiempo, se produce una colisión. Cuando se produce una colisión la trama transmitida se elimina y se envía una señal de embotellamiento a todos los nodos del segmento. Los nodos esperan un período de tiempo al azar y luego vuelven a enviar los datos. Las colisiones excesivas pueden reducir el ancho de banda disponible de un segmento de red del 35% al 40%.

2.1.4.3 Segmentación

La segmentación se realiza cuando un sólo dominio de colisión se divide en dominios de colisión más pequeños. Los dominios de colisión más pequeños reducen la cantidad de colisiones en un segmento LAN y permiten una mayor utilización del ancho de banda. Los dispositivos de la Capa 2 como por ejemplo puentes y switches se pueden utilizar para segmentar una LAN. Los routers pueden lograr esto a nivel de la Capa 3.

El MAG contará con varios dominios de colisión determinados por los elementos activos empleados en la capa de acceso y distribución del modelo SAFE.

2.1.4.4 Dominio de broadcast

Se produce un broadcast cuando el control de acceso al medio destino (MAC) se configura en FF-FF-FF-FF-FF-FF. Un dominio de broadcast se refiere al conjunto de dispositivos que reciben una trama de datos de broadcast desde cualquier dispositivo dentro de este conjunto. Todos los hosts que reciben una trama de datos de broadcast deben procesarla. Este proceso consume los recursos y el ancho de banda disponible de la red. Los dispositivos de Capa 2 como los puentes y switches reducen el tamaño de un dominio de colisión pero no reducen el tamaño del dominio de broadcast. En cambio los ruteadores reducen el tamaño del dominio de colisión y el tamaño del dominio de broadcast a través del uso del direccionamiento IP que se realiza en la capa 3.

Los ruteadores son dispositivo de capa 3, se pueden usar para crear segmentos de LAN únicos, también para segmentar la LAN en redes lógicas y físicas exclusivas y permitiendo conectividad a las WAN.

El enrutamiento de capa 3 determina el flujo de datos entre los segmentos de red conectados al ruteador, para lo cual se utilizan las direcciones de capa 3 (IP), un ruteador envía paquetes de datos basados en direcciones destino. La interfaz del ruteador es el punto de entrada y salida de un dominio de broadcast, y evita que los broadcast lleguen hasta los otros segmentos LAN. Los ruteadores ofrecen escalabilidad, dado que sirven como cortafuegos para los broadcast y pueden dividir las redes en subredes pero son más caros y mas difícil de configurar que un switch.

En la figura 2.2 se describe gráficamente los conceptos de dominio de colisión y dominio de broadcast explicados anteriormente.

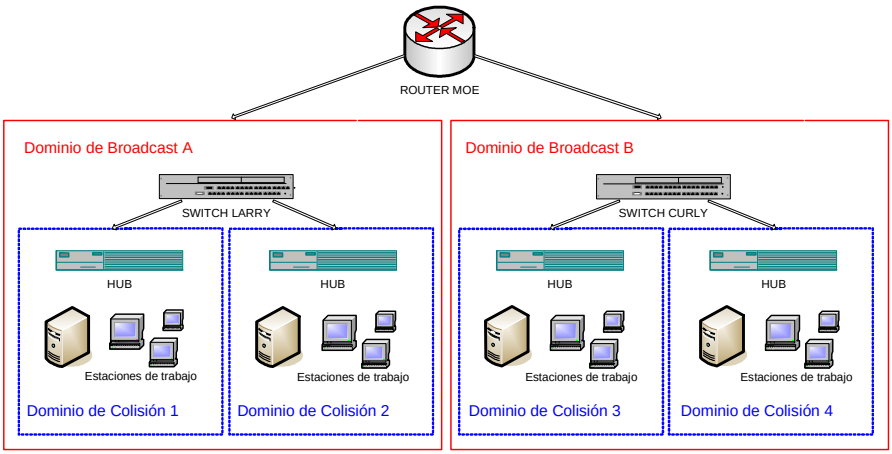


Fig. 2.2 Dominios de Colisión y Dominios de Broadcast.

El MAG contará con ruteadores para enlazar las VLAN´s que se crearán como se explica mas adelante.

3.1.5 APLICACIÓN DE LA METODOLOGÍA SAFE EN EL DISEÑO DE LA RED DEL MAG.

La metodología que se utilizará para el diseño de la red del Ministerio es la sugerida por Cisco, que considera un modelo de diseño jerárquico basado en una topología física en estrella extendida, además que es la topología existente en este momento en el Ministerio.

2.1.5.1 Modelo de diseño jerárquico

El uso de un modelo de diseño jerárquico facilitará los cambios de la red a medida que crezca la organización. Un modelo de diseño jerárquico incluye las siguientes tres capas:

- La Capa de Acceso: Proporciona acceso a la red a los usuarios del Ministerio.
- La Capa de Distribución: Brinda conectividad basada en políticas.
- La Capa de Núcleo: Proporciona transporte óptimo entre sitios.

1.1.5.1.1 Capa de Acceso

Es el punto de entrada para los host del Ministerio, en esta capa se encuentran involucradas la capa 1 y 2 del modelo OSI. Los switches de la capa de acceso operan en la capa 2 del modelo OSI, ofrecen servicios como asociación de

VLAN´s y su principal propósito es proporcionar a los usuarios finales acceso a la red.

En esta capa de acceso se encuentran los llamados IDF´s (Intermedio Distribution Floor) que concentrarán a los usuarios de las distintas dependencias y de la Administración Central del MAG y que por lo general se ubican uno en cada piso excepto en los pisos donde existe gran cantidad de hosts o varias dependencias.

Basándonos en el número de usuarios determinados en el capítulo 1 y en la ubicación por pisos de las distintas dependencias y de la Administración del MAG, podemos determinar los IDF´s y número de switches de capa de acceso necesarios en cada uno de los pisos del Ministerio, obteniendo como resultado la tabla 2.2 que se muestra a continuación, en esta tabla no están todos los switchs requeridos para conectar a todos los hosts ya que también se conectan en los switchs de capa distribución explicados mas adelante.

PISO	DEPENDENCIA	USUARIOS		IDF´s	SWITCHS	CANTIDAD
		EXISTENTES	ESTIMADOS			
12	MAG	67	90*	IDF1	24 puertos	1
11	MAG	64	90*	IDF2	48 puertos	1
10	MAG	45	45*	IDF3		
10	MAG(Coop. Inter)	21	30*	IDF11	24 puertos	2
10	PRAT	20	20*	IDF3	24 puertos	1
9	SESA	79	84*	IDF5	24 puertos 48 puertos	2 1
9	CADERS	75	90*	IDF6	24 puertos	3
9	MAG	21	21*	IDF12	24 puertos	1
6	INCCA	22	23*	IDF7	24 puertos	1
6	MAG	79	90*	MDF	24 puertos 48 puertos	4 1
5	MAG	76	90*	IDF4/MDF	24 puertos	1
4	INIAP	21	21*	IDF10	24 puertos	1
3	CNRH	65	85*	IDF8	24 puertos	3
PB	MAG	14	20*	IDF9	24 puertos	1

* Crecimiento estimado de usuarios según los administradores de las redes.

Tabla 2.2 Cantidad de IDF´s y Switchs en la capa de Acceso

1.1.5.1.2 Capa de Distribución

La capa de distribución se encuentra entre las de acceso y núcleo, su propósito es ofrecer una definición fronteriza en la cual se pueda llevar a cabo la manipulación de paquetes.

Los switches en esta capa operan en la capa 2 del modelo OSI, las funciones de la capa de distribución en una red conmutada es unificar las conexiones de los IDF´s, definir los dominios de broadcast, enrutamiento de VLAN´s, seguridad, etc.

Los switches de la capa de distribución son los puntos de totalización de múltiples switches de la capa de acceso, debe tener un alto rendimiento, ya que es el punto en el que se encuentra delimitado el dominio de broadcast. La capa de distribución combina el tráfico VLAN y es un punto focal para las decisiones de política de flujo de tráfico, combinan las funciones de un router y un switch en un dispositivo, diseñados para conmutar el tráfico y obtener rendimiento mayor que un ruteador estándar.

En esta capa de distribución se encuentran también los IDF´s que enlazarán la capa de acceso con la capa núcleo, en estos IDF´s también pueden instalarse los servidores de grupo permitiendo al tráfico viajar por la infraestructura de red hacia un IDF y no afectar a los demás usuarios en ese segmento de red.

Nuevamente basándonos en el número de usuarios determinados en el capítulo 1 y en la ubicación por pisos de las distintas dependencias y de la Administración del MAG, podemos determinar los IDF´s y número de switches de capa de distribución necesarios en cada uno de los pisos del Ministerio, obteniendo como resultado la tabla 2.3 que se muestra a continuación:

PISO	DEPENDENCIA	USUARIOS		IDFs	SWITCHS	CANTIDAD
		EXISTENTES	ESTIMADOS			
12	MAG	67	90*	IDF1	48 puertos + 2 de fibra	2
11	MAG	64	90*	IDF2	48 puertos + 2 de fibra	1
10	MAG	45	45*	IDF3	48 puertos + 2 de fibra	1
9	CADERS	75	90*	IDF6	48 puertos + 2 de fibra	1
6	CADERS	26	26*	IDF13	48 puertos + 2 de fibra	1
6	MAG	79	90*	MDF	48 puertos + 2 de fibra	1
3	CNRH	65	85*	IDF8	48 puertos + 2 de fibra	1

* Crecimiento estimado de usuarios según los administradores de las redes.

Tabla 2.3 Cantidad de IDF´s y Switches en la Capa de Distribución

1.1.5.1.3 Capa Núcleo.

Esta capa no debe realizar ninguna manipulación de paquetes, como filtrado de listas de acceso, controlar la conmutación de paquetes, etc. solo pasa paquetes lo más rápido que se pueda.

Una infraestructura central con rutas alternadas redundantes ofrece estabilidad a la red en caso de falla.

Los switches de la capa núcleo son el backbone de la red conmutada de campus, si no tienen un módulo de router asociado se usa un router externo para la función de capa 3, los switches de esta capa pueden hacer uso de una serie de tecnologías de capa 2 como ethernet, conmutación de celdas, ATM, etc.

En esta capa de núcleo se encuentra el MDF (Main Distribution Floor), los servidores empresariales deben colocarse en este MDF. Siempre que sea posible, el tráfico hacia los servidores empresariales sólo tiene que viajar hacia el MDF y no transmitirse a través de otras redes.

Basándonos en el criterio de que el MDF debe encontrarse lo mas cerca al departamento de Informática y como este se halla en el piso 6, el MDF lo colocaremos en dicho piso.

En este MDF se colocará el único switch core que utilizaremos en la implementación.

Luego de concluir este análisis y basándonos también en el primer capitulo, podemos resumir los requerimientos de la red del Ministerio mostrados en la tabla 2.4 y el resumen de los elementos activos necesarios para la red del Ministerio también mostrados en la tabla 2.5.

REQUERIMIENTO	DESCRIPCIÓN	MOTIVO
NÚMERO DE USUARIOS	MAG 456 PRAT 20 SESA 84 CADERS 110 INCCA 23 INIAP 21 CNRH 85	Número de usuarios estimados con crecimiento.
OPERACIONES CRÍTICAS	Acceso a Internet desde cualquier estación de trabajo y funciones administrativas que utilizan la red	
VELOCIDAD DE TRANSMISIÓN	10BASE-T, 100BASE-TX, 100BASE-FX Y 1000BASE-FX	Son las velocidades estándar.
TOPOLOGIA FÍSICA	ESTRELLA EXTENDIDA	Es la topología existente y por ser la más usada.
TECNOLOGÍA	IEEE 802.3	Es la usada en esta topología
ACCESO AL MEDIO	CSMA/CD	Es la usada en esta tecnología.
TIPO DE CABLE	COBRE Y FIBRA ÓPTICA	Es lo usado para estas redes.
PROTOCOLOS	TCP/IP	Es el protocolo existente y de uso común.
NORMA	EIA/TIA 568	Es la norma existente.
PLATAFORMA	WINDOWS	Es la plataforma existente.

Tabla 2.4 Cuadro de requerimientos de la red del Ministerio

IDF	NÚMERO SWITCHS	USUARIOS EXISTENTES	USUARIOS ESTIMADOS	PUERTOS MÁXIMOS	PUERTOS DE FIBRA	P. COBRE GIGABIT
1	3	67	90	96	2	0
2	2	64	90	96	1	0
3	2	65	65	72	1	0
4	1	20	20	24	0	1
5	3	79	80	96	1	0
6	4	75	90	120	2	0
7	1	23	23	24	0	0
8	4	65	85	120	1	2
9	1	14	20	24	1	0
10	1	21	21	24	0	0
11	2	21	30	48	0	0
12	1	21	21	24	0	0
13	1	20	20	48	0	0
MDF	7	135	160	192	9	1

Tabla 2.5 Resumen del diseño de la red del Ministerio

2.1.5.2 Diseño Lógico

El diseño lógico de la red se refiere al flujo de datos que hay dentro de una red, también se refiere a los esquemas de nombre y dirección que se utilizan en la implementación del diseño de la red. El diagrama lógico es una visión general

instantánea de toda la implementación de la LAN, es útil para el diagnóstico de fallas y para implementar la expansión en el futuro.

El diagrama lógico es el mapa de ruta básico de la red que incluye los siguientes elementos:

- Especificar las ubicaciones e identificaciones de los armarios de cableado MDF e IDF.
- Documentar el tipo y la cantidad de cables que se utilizan para interconectar los IDF con el MDF.
- Documentar la cantidad de cables de repuesto que están disponibles para aumentar el ancho de banda entre los armarios de cableado.
- Proporcionar documentación detallada sobre todos los tendidos de cable, los números de identificación y en cuál de los puertos del HCC (Conexión Cruzada Horizontal) o VCC (Conexión Cruzada Vertical) termina el tendido de cableado.

Tomando en cuenta los aspectos anteriores, en la figura 2.3 se presenta el diagrama lógico de capa 1 de la red del Ministerio.

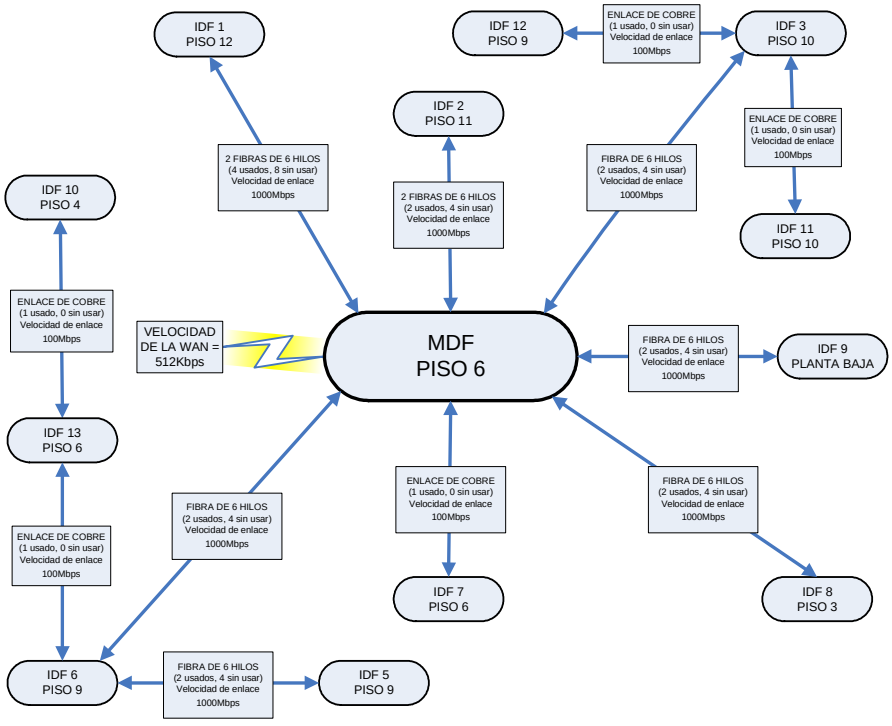


Fig. 2.3 Diagrama lógico de capa 1 del Ministerio

A continuación en las tablas 2.6 y 2.7 se detallan las identificaciones de los cables de Backbone y de los puertos del HCC y los VCC:

	MDF	IDF5	IDF10	IDF11	IDF12	IDF13
MDF						
IDF1	FX-1					
IDF2	FX-2					
IDF3	FX-3			TX-3-11	TX-3-12	
IDF4	TX-4					
IDF5						
IDF6	FX-6	FX-6-5				TX-6-13
IDF7	TX-7					
IDF8	FX-8					
IDF9	FX-9					
IDF10						
IDF11						
IDF12						
IDF13			TX-13-10			

Tabla 2.6 Identificación de cables de backbone

Nomenclatura
FX = Fibra Óptica
TX = Par Trenzado

	MDF	IDF5	IDF10	IDF11	IDF12	IDF13
MDF						
IDF1	BB M-1					
IDF2	BB M-2					
IDF3	BB M-3			BB 3-11	BB 3-12	
IDF4	BB M-4					
IDF5						
IDF6	BB M-6	BB 6-5				BB 6-13
IDF7	BB M-7					
IDF8	BB M-8					
IDF9	BB M-9					
IDF10						
IDF11						
IDF12						
IDF13			BB 13-10			

Tabla 2.7 Identificación en los puertos del HCC y los VCC

Nomenclatura
BB xx-yy = Backbone extremo-extremo
M = MDF
# = IDF

3.1.6 DISEÑO DE SEGURIDAD

Para la seguridad periférica se implementará un Firewall que proteja a la red del Ministerio de ataques externos, creando tres zonas claramente definidas que son la Outside que es la salida hacia el Internet, la Inside que es la red interna del ministerio la misma que tiene que estar protegida de los ataques, y la zona desmilitarizada o DMZ que es donde están los equipos que acceden desde afuera y prestan servicios a la red interna.

Los servidores que formarán parte de la DMZ son: El de base de datos del INCCA, el Webserver del MAG, el de base de datos del MAG y el servidor de Agroecuador.

Luego de tener el diseño lógico de la red de datos del Ministerio, ya podemos elaborar un diagrama físico de la red sin tomar en cuenta la seguridad periférica que se la detallará mas adelante, y esta quedaría como se indica en la figura 2.4.

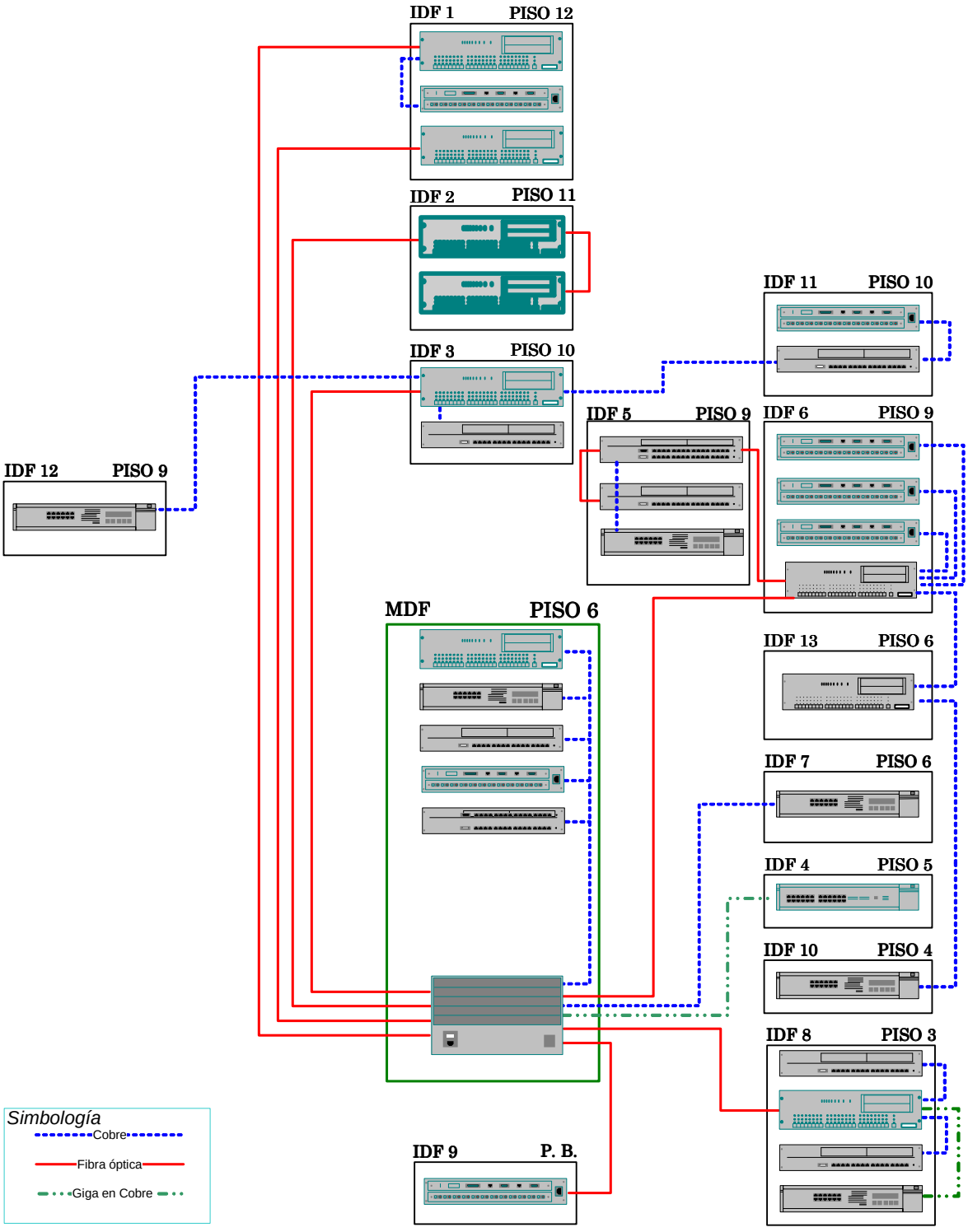


Fig. 2.4 Diagrama físico de la red del Ministerio

3.2 DISEÑO DE VLAN´S

3.2.1 CONCEPTO DE VLAN

Una VLAN es un agrupamiento lógico de dispositivos o usuarios independientemente de su ubicación física en un segmento de red, de tal modo que se puedan comunicar como si estuvieran conectados al mismo medio, cuando en realidad, están ubicados en distintos segmentos de la LAN. Se pueden agrupar por función, departamento o aplicación. La configuración de las VLAN´S se hace en los switches mediante software.

3.2.2 CARACTERÍSTICAS PRINCIPALES

Las VLAN´S presentan las siguientes características:

- Las VLAN´S funcionan en la Capa 2 y Capa 3 del modelo de referencia OSI.
- La comunicación entre las VLAN´S es implementada por el enrutamiento de Capa 3.
- Las VLAN´S proporcionan un método para controlar los Broadcasts de red.
- El administrador de la red asigna usuarios a una VLAN y es mucho más fácil administrarlas y asignar recursos.
- Las VLAN´S pueden aumentar la seguridad en la red, definiendo cuales son los nodos de red que se pueden comunicar entre si y la comunicación entre VLAN´s se puede hacerse a través de routers, los cuales pueden introducir filtros mucho más especializados.

3.2.3 FORMAS DE IMPLEMENTACIÓN DE VLAN´S

Existen tres maneras más importantes de implementar VLAN´S que son las siguientes:

- Por puerto. Son las mas comunes, cada puerto de un switch puede soportar una sola VLAN, aquí los protocolos capa 3 no son filtrados. Para comunicarse entre VLAN´s se necesita un router externo. A este tipo de VLAN se le conoce como *segment based VLAN.*
- Por protocolo. En este caso una VLAN está basada en direcciones de red (OSI nivel 3) puede diferenciar entre diferentes protocolos, El ruteo entre VLAN´S se hace internamente, sin necesidad de un router externo. Ya no son

comunes debido al DHCP. Este tipo de VLAN´s se conoce como *virtual subnet VLAN*.

- Por direcciones MAC. Se implementan con escasa frecuencia, hay que introducir y configurar cada dirección en forma individual, ofrece flexibilidad pero aumenta el gasto.

3.2.4 MECANISMOS DE ENLACE ENTRE VLAN´S

Existe un mecanismo que se utiliza para enlazar VLAN´S que es el TRUNKING, los puertos trunk habilitan conexiones entre switches para llevar tráfico perteneciente a múltiples VLAN´s, entre dispositivos sobre el mismo enlace. Un dispositivo puede determinar a que VLAN pertenece un tráfico en base al VLAN ID (VLAN identifier), que es una etiqueta que está encapsulada con el dato. El estándar de la IEEE, 802.1Q, es un tipo de encapsulamiento usado para llevar datos de múltiples VLAN´s sobre enlaces trunk. Otros mecanismos son el ISL (enlace inter-Switch) que es propiedad de Cisco y el LAN Emulation, utilizado en Backbone ATM, los cuales ya no son utilizados.

3.2.5 CONTROL DE FLUJO ENTRE VLAN´S

En algunas situaciones, resulta interesante unir dos LAN con más de un router, pero esto puede ocasionar que se produzcan ciclos sin fin haciendo que las redes se saturen, para evitar este problema existe un mecanismo que permite a los routers comunicarse entre sí, pasándose información sobre la topología de las conexiones existentes. Una vez conocida la topología los routers desactivarán las conexiones redundantes para garantizar que haya un único camino uniendo todas las redes, de forma que se evite la creación de loops. Las conexiones que lógicamente se pongan fuera de servicio quedarán listas para entrar en funcionamiento si las conexiones activas fallan por algún motivo. El algoritmo se repite cada cierto tiempo, por lo que si alguno de los enlaces queda fuera de funcionamiento por algún motivo en la siguiente ronda se habilitará algún camino alternativo que lo sustituya. El protocolo que permite esto se conoce como Spanning Tree o STP, y forma parte de la especificación IEEE 802.1d.

Este protocolo también se utiliza en la unión de VLAN´S conectadas a diferentes switches.

3.2.6 DISEÑO DE VLAN´S

Todo proceso de desarrollo e implantación tecnológico requiere una etapa previa de diseño que permita identificar la situación, determinar los requerimientos y establecer las condiciones que permitirán el cumplimiento de lo requerido.

En un inicio las VLAN´S se les agrupaba basándose en la clasificación administrativa sin importa su ubicación y se las llamaba de extremo a extremo, los host agrupados deben tener los mismos patrones de flujo de tráfico como 80/20 que quiere decir 80% del tráfico contenido en la VLAN y el 20% restante atraviesa el router a los servidores, a la Internet y a la WAN, cada VLAN tiene un conjunto común de requisitos de seguridad para todos los miembros.

En la actualidad el concepto de agrupación a cambiado. A medida que se busca centralizar recursos, es mas difícil mantener una VLAN de extremo a extremo, se requiere que los usuarios usen varios recursos que puede que no estén en sus VLAN´S. El cambio en la asignación y uso de recursos requiere que se creen las VLAN en torno de límites geográficos y de aquí su nombre VLAN´S geográficas, en lugar de límites de aspectos comunes. Esta ubicación geográfica puede ser tan grande como un edificio entero o como un solo switch, En una estructura geográfica es típico la nueva norma 20/80, 20% del tráfico permanece dentro de la VLAN y el 80% viaja fuera de la VLAN, esta topología implica que los servicios desde los recursos deben viajar a través de un dispositivo de capa 3, este diseño permite que la red aplique un método determinado y coherente para acceder a los recursos.

Para el diseño de las VLAN´S del Ministerio se tomarán en cuenta los dos conceptos anteriores, se agruparán por dependencias y también geográficamente, como se indica en la tabla 2.8 siguiente:

VLAN	INTEGRANTES	JUSTIFICACIÓN
1	Todos lo miembros de la administración del MAG.	Servicios y aplicaciones comunes del MAG.
2	Las dependencias adscritas, PRAT, INCCA, INIAP, CNRH.	Servicios y aplicaciones comunes de las dependencias adscritas.
3	Todos los equipos del centro de cómputo, capacitación y los equipos activos.	Seguridad.
4	Los equipos de la zona desmilitarizada	Seguridad.
5	Los equipos del SESA	Servicios y aplicaciones comunes del SESA.
6	Los equipos del CADERS	Servicios y aplicaciones comunes del CADERS.

Tabla 2.8 Primera distribución de VLAN´S

Desde la VLAN 2 a la VLAN 6 según el diseño anterior se estima que los usuarios no pasarán de 200, pero en la VLAN 1 los usuarios son más de 400 y como se usarán redes o subredes clase C donde los usuarios no pasan de 254 como se explica mas adelante, se reparten los usuarios de la VLAN1 en la VLAN 2 ya que los servicios y las aplicaciones de estas VLAN´s son similares.

3.3 ESPECIFICACIONES DE DIRECCIONAMIENTO IP

3.3.1 DIRECCIONAMIENTO IP

IP constituye el protocolo de direccionamiento de la suite de protocolos TCP/IP. Su función está orientada a proveer direccionamiento en el nivel de red e identificación de redes y Hosts. Esta es la razón por la que IP es la base para el enrutamiento de los paquetes en una red y da una identificación global y única de los elementos de la red.

Las direcciones IP tienen una longitud de 32 bits y constan de dos partes: La dirección de Red y la dirección de Host. Cada byte de la dirección IP es representado por un número decimal de 0 a 255 separados por un punto. Por ejemplo: 172.16.25.10.

Las direcciones IP se clasifican en Direcciones Públicas y Privadas. Las Públicas son visibles desde todo Internet, se deben contratar a un ISP o al Registro Americano de Números de Internet (ARIN). Las Direcciones Privadas son utilizadas para identificar a los hosts dentro de una red interna (local) y no son visibles desde el Internet.

Las direcciones de red Privadas se muestran en Tabla 2.9.

Clase	Redes
A	10.0.0.0 hasta 10.255.255.255
B	172.16.0.0 hasta 172.31.0.0
C	192.168.0.0 hasta 192.168.255.0

Tabla 2.9. Rangos de direcciones IP Privadas

Las direcciones IP pueden ser Direcciones Estáticas cuando un host se conecta a la red con una misma dirección y Direcciones Dinámicas cada vez que un host se conecta a una red lo hace con una dirección IP distinta.

La dirección de red es la parte de la dirección IP utilizada para nombrar a la red. El enrutamiento de paquetes se lo hace tomando como referencia precisamente la dirección de red.

La dirección de Host se utiliza para diferenciar cada elemento de la red que posea una dirección MAC. Esto es “todos los elementos de una red, poseen una dirección que los identifica ante los demás de su misma red llamada dirección de Host”. Los PCs, Servidores, Switch, Routers, entre otros, son ejemplos de Host, y por tanto deben ser direccionados. En otras palabras, todo equipo que necesite enviar y recibir datagramas o paquetes IP, se debe identificar con una dirección IP.

3.3.2 CLASES DE DIRECCIONES IP.

Su estructura se basa en un concepto jerárquico único. Un lema a tener en cuenta a la hora de definir que direcciones IP se debe asignar, es “Las direcciones IP son un recurso lógico limitado”. Las clases de direcciones sirven

para definir los bits de la dirección IP que se van a destinar para red y Host de acuerdo a las cantidades requeridas por cada uno.

Las clases de direcciones que nos interesa para nuestro estudio son: A, B y C.

Clase A:

Asigna el primer octeto (8 bits) para direccionar redes y los tres octetos restantes (24 bits) para Host. Con este esquema se pueden direccionar hasta 16.777.214 Host y 126 redes. Si el primer bit de una dirección IP es 0, esta pertenece a una red de clase A, el rango que comprende estas direcciones es 1.0.0.0 a 126.0.0.0

Esta clase, por las pocas direcciones de red que maneja, es bastante utilizada en redes WAN, donde generalmente se tienen pocas redes pero gran cantidad de Host.

Clase B:

Esta clase asigna equitativamente los bits para red y Host. 16 bits para redes y 16 bits para Host. Bajo este esquema se pueden direccionar 65.534 Host y 16.256 redes. El rango para clase B es el siguiente: 128.1.0.0 a 191.254.0.0. Esta clase es una de las más utilizadas para Internet, por su capacidad de direccionar gran cantidad de redes. Si los primeros dos bits de una dirección son 10, esta es una dirección de clase B.

Clase C:

Esta clase funciona en la distribución de bits, en forma contraria a la clase A, separa los primeros 24 bits para red y los 8 restantes para Host. Con este esquema se tienen 2.072.640 redes y 254 Host por cada red. El rango para esta clase es desde 192.0.1.0 a 223.255.255.0. Si los tres primeros bits de una dirección IP son 110, esta es una dirección de clase C.

Existen otras clases que no son de dominio público. Su utilización está restringida a entidades privadas de investigación. Clase D es para multicasting (servicios de difusión múltiple de datos), su rango está entre 224.0.0.0 y 239.255.255.254. La clase E es de investigación

Los valores 0 y 127 del primer byte son de uso especial, 0 es para el direccionamiento de default y 127 para el direccionamiento de Loopback. La dirección por default es usada para simplificar la información de encaminamiento que es manejada por el protocolo IP. La dirección de Loopback se utiliza para pruebas del TCP/IP y para la comunicación de procesos internos cuando la misma máquina es el destino.

Existen algunas direcciones de Host que tienen usos especiales, en todas las clases de redes, las direcciones de Host 0 y 255 son reservadas. Una dirección IP con todos los bits de la parte de Host puestos a cero, representan a la red en si misma. Una dirección IP con todos los bits de la parte de Host puestos en uno es una dirección de broadcast que es usada para direccionar simultáneamente a todas las máquinas dentro de una red.

En la tabla 2.10 se puede resumir las clases de redes y sus valores.

Tabla 2.10 Clases de redes y sus valores.

Clase de red	Bits del 1er Byte	Rango del 1er Byte	Formato de la dirección	Número de redes	Número de Host por red
A	0xxxxxxx	1 – 126	R.H.H.H	$2^7 – 2$*	$2^{24} – 2$**
B	10xxxxxx	128 – 191	R.R.H.H.	2^{14}	$2^{16} – 2$**
C	110xxxxx	192 – 223	R.R.R.H.	2^{21}	$2^8 – 2$**
D	1110xxxx	224 – 239			
E	11110xxx	240 – 247			

* (0 y 127 son de uso especial)

** (IP de red, IP de Broadcast)

3.3.3 MÁSCARA DE RED.

Sirve para identificar la red a la cual pertenece una dirección IP. Una operación lógica binaria AND entre la dirección IP y la máscara dará como resultado el valor de la red. En la máscara se utiliza “1s” para identificar redes y “Os” para identificar Host. La máscara también permite determinar el número de subredes que contiene una red.

Otra forma común para referirnos a la máscara es decir cuantos bits “1s” tiene. Por ejemplo la máscara de la clase A es de 8 bits (/8), clase B 16 bits (/16) y clase C 24 bits (/24). Classless Interdomain Routing CIDR es un método de representación de una dirección IP y su máscara mediante un prefijo, por ejemplo: 192.168.50.0/24, 24 es el número de 1s en la máscara de subred, es decir 255.255.255.0.

Si la dirección de un Host es 172.16.32.35 y la máscara es 255.255.0.0, realizando un AND tenemos:

	172.	16.	32.	35	Dirección
AND	255.	255.	0.	0	Máscara
	172.	16.	0.	0	Red

La máscara para una red de clase A es 255.0.0.0, para una red de clase B es 255.255.0.0 y para una red de clase C es 255.255.255.0, estas máscaras se refieren a redes que no contienen subredes.

3.3.4 ASIGNACIÓN DE IP´s AL MINISTERIO.

Al ministerio le han sido asignadas las siguientes direcciones IP´s públicas clase C:

201.234.200.193
201.234.200.194
201.234.200.195
201.234.200.196
201.234.200.197
201.234.200.198

En cuanto a la asignación de direcciones privadas, podemos observar en el diseño de VLAN´s, que la VLAN 1 y la VLAN 2 son las que más host van a tener por lo que se decide utilizar direcciones IP Clase B, en cambio para las VLAN´s 3, 4, 5 y 6, se usarán direcciones IP Clase C, quedando como indica la tabla 2.11.

VLAN	DIRECCIÓN DE RED	MASCARA
1	172.16.0.0	255.255.0.0
2	172.16.0.0	255.255.0.0
3	192.168.254.0	255.255.255.0
4	192.168.252.0	255.255.255.0
5	192.168.5.0	255.255.255.0
6	192.168.1.0	255.255.255.0

Tabla 2.11 Direcciones de red de las VLAN´s

3.4 ESPECIFICACIONES DE SUBREDES

3.4.1 DEFINICIONES BÁSICAS

Como se había dicho, las direcciones IP son un recurso limitado y costoso cuando se utilizan en Internet, por consiguiente no hay que desperdiciar direcciones al momento de armar el plan de direccionamiento.

Las subredes es una forma de administrar adecuadamente las direcciones IP, y consiste en tomar bits de izquierda a derecha de los destinados originalmente para Host y convertirlos en bits de red transformándolos en “1s”.

Para conocer como definir una dirección de subred, se debe tomar en cuenta el número de subredes que se desea obtener e igualar a la expresión 2 elevado a la n. Este número n servirá luego para realizar un desplazamiento de la línea de división entre los bits de la parte de red hacia los bits de la parte de Host.

A continuación se presenta un ejemplo: Una red de clase A dividir en 8 subredes, encontrar la máscara, la IP de subred y el broadcast.

Red de clase A

IP de red	88	0	0	0
	1011000	00000000	00000000	00000000
Máscara	255	0	0	0
	11111111	00000000	00000000	00000000

Máscara para 8 subredes

Número de subredes = 2^n

$8 = 2^3$
n = 3 número de bits que vamos a quitar al Host

11111111 . 11100000 . 00000000 . 00000000
255 . 224 . 0 . 0

IP de subred 1:	1011000	00000000	00000000	00000000
	88	0	0	0
Broadcast subred 1:	1011000	00011111	11111111	11111111
	88	31	255	255
IP de subred 2:	1011000	00100000	00000000	00000000
	88	32	0	0
Broadcast subred 2:	1011000	00111111	11111111	11111111
	88	63	255	255
IP de subred 3:	1011000	01000000	00000000	00000000
	88	64	0	0
Broadcast subred 3:	1011000	01011111	11111111	11111111
	88	95	255	255
IP de subred 4:	1011000	01100000	00000000	00000000
	88	96	0	0
Broadcast subred 4:	1011000	01111111	11111111	11111111
	88	127	255	255
IP de subred 5:	1011000	10000000	00000000	00000000
	88	128	0	0
Broadcast subred 5:	1011000	10011111	11111111	11111111
	88	159	255	255
IP de subred 6:	1011000	10100000	00000000	00000000
	88	160	0	0
Broadcast subred 6:	1011000	10111111	11111111	11111111
	88	191	255	255
IP de subred 7:	1011000	11000000	00000000	00000000
	88	192	0	0
Broadcast subred 7:	1011000	11011111	11111111	11111111
	88	223	255	255
IP de subred 8:	1011000	11100000	00000000	00000000
	88	224	0	0
Broadcast subred 8:	1011000	11111111	11111111	11111111
	88	255	255	255

Otra forma de administrar adecuadamente las direcciones IP ignorando la antigua distinción entre clases de direcciones al igual que las subredes, es el nuevo

sistema denominado encaminamiento sin clases (classless routing). Esta denominación conllevó que el sistema original fuera denominado encaminamiento con clases (classful routing).

Classless Inter-Domain Routing (CIDR Encaminamiento Inter-Dominios sin Clases) se introdujo en 1993 y representa la última mejora en el modo como se interpretan las direcciones IP.

CIDR facilita el encaminamiento al permitir agrupar bloques de direcciones en una sola entrada de tabla de rutas. Estos grupos, llamados comúnmente Bloques CIDR, comparten una misma secuencia inicial de bits en la representación binaria de sus direcciones IP.

Los bloques CIDR se identifican usando una sintaxis similar a la de las direcciones IP: cuatro números decimales separados por puntos, seguidos de una barra de división y un número de 0 a 32; A.B.C.D/N.

Los primeros cuatro números decimales se interpretan como una dirección IP, y el número tras la barra es la longitud de prefijo, contando desde la izquierda, y representa el número de bits comunes a todas las direcciones incluidas en el bloque CIDR.

00001010 . 00001010 . 00000001 . 00100000 10.10.1.32/27
00001010 . 00001010 . 00000001 . 00101100 10.10.1.44/27

Decimos que una dirección IP está incluida en un bloque CIDR, y que encaja con el prefijo CIDR, si los N bits iniciales de la dirección y el prefijo son iguales. Por tanto, para entender CIDR es necesario visualizar la dirección IP en binario. Dado que la longitud de una dirección IP es fija, de 32 bits, un prefijo CIDR de N-bits deja 32 − N bits sin encajar, y hay $2^{(32 - N)}$ combinaciones posibles con los bits restantes. Esto quiere decir que $2^{(32 - N)}$ direcciones IP encajan en un prefijo CIDR de N-bits.

CIDR usa máscaras de subred de longitud variable (VLSM, Variable Lenght Subnet Mask) para asignar direcciones IP a subredes de acuerdo a las necesidades de cada subred. De esta forma, la división red/host puede ocurrir en

cualquier bit de los 32 que componen la dirección IP. Este proceso puede ser recursivo, dividiendo una parte del espacio de direcciones en porciones cada vez menores, usando máscaras que cubren un mayor número de bits.

VLSM parte del mismo concepto que CIDR. El término VLSM se usa generalmente cuando se habla de redes privadas, mientras que CIDR se usa cuando se habla de Internet (red pública).

3.4.2 DEFINICIÓN DE SUBREDES PARA EL MINISTERIO

Para el caso de las redes del Ministerio, se subnetearán las VLAN´s 1 y 2 que son redes clase B, de tal forma que el número de host por subred sea de 254.

VLAN 1

Red clase B

IP de red	172	16	0	0
	10101100	00010000	00000000	00000000
Máscara	255	255	0	0
	11111111	11111111	00000000	00000000

Máscara para 256 subredes
Número de subredes = 2^n
$256 = 2^8$
n = 8 número de bits que vamos a quitar al Host

11111111 . 11111111 . 11111111 . 00000000
255 . 255 . 255 . 0

IP de subred 30:	10101100	00010000	00011101	00000000
	172	16	29	0
Broadcast subred 30:	10101100	00010000	00011101	11111111
	172	16	29	255

VLAN 2

Red clase B

IP de red	172	16	0	0
	10101100	00010000	00000000	00000000
Máscara	255	255	0	0
	11111111	11111111	00000000	00000000

Máscara para 256 subredes
Número de subredes = 2^n
$256 = 2^8$
n = 8 número de bits que vamos a quitar al Host

11111111 . 11111111 . 11111111 . 00000000
255 . 255 . 255 . 0

IP de subred 29:	10101100	00010000	00011100	00000000
	172	16	28	0
Broadcast subred 29:	10101100	00010000	00011100	11111111
	172	16	28	255

Para el caso de las VLAN´s 3, 4, 5 y 6 no se subneteará ya que son redes clase C y necesitamos las 254 direcciones de host en cada VLAN.

3.5 ESPECIFICACIONES DE ENRUTAMIENTO

El enrutamiento es el mecanismo por el cual se determinan las trayectorias más óptimas a través de una red con el menor retardo y la mayor fiabilidad posible.

Asociado al enrutamiento existe el concepto de métrica, que es una medida de lo "bueno" que es usar un camino determinado. La métrica puede estar asociada a distintas magnitudes: distancia, costo, retardo de transmisión, número de saltos, etc., o incluso a una combinación de varias magnitudes. Lo ideal en una red es conseguir el enrutamiento más óptimo. Típicamente el enrutamiento es una función implantada en la capa 3(capa de red) del modelo de referencia OSI.

En los protocolos de enrutamiento existen dos grandes categorías que son los internos (Interor Gateway Protocols, IGP) que son los que funcionan dentro de un sistema autónomo y los externos (Exterior Gateway Protocol, EGP) que son los que conectan diferentes sistemas autónomos entre sí.

Los algoritmos que se pueden usar en una red para la función de enrutamiento pueden ser de dos tipos, enrutamiento estático o no adaptativo y enrutamiento dinámico o adaptativo.

3.5.1 ENRUTAMIENTO ESTÁTICO O NO ADAPTATIVO

No tienen en cuenta el estado de la red al tomar las decisiones de encaminamiento. Las tablas de encaminamiento de los nodos se configuran de forma manual y permanecen inalterables hasta que no se vuelve a actuar sobre ellas. Por tanto, la adaptación en tiempo real a los cambios de las condiciones de la red es nula.

3.5.2 ENRUTAMIENTO DINAMICO O ADAPTATIVO

Es cuando los ruteadores de la red toman decisiones basándose en las condiciones actuales de la red. Estos algoritmos permiten que la red se adapte a condiciones cambiantes en la misma. Por ejemplo, si un enlace deja de estar operativo, un algoritmo dinámico acaba reaccionando ante esa condición y cambia las rutas para que no utilicen el enlace que ya no funciona.

Los algoritmos dinámicos son los preferidos en la mayoría de las redes debido a su capacidad de responder a cambios en el estado de la red. Los algoritmos dinámicos básicos más utilizados son vector distancia y estado del enlace.

Vector distancias:

Se basa en que un ruteador se comunica con sus vecinos indicándoles qué distancias estima hacia los nodos de toda la red. Con la información que un nodo recibe de sus vecinos, puede estimar cuáles son los caminos óptimos. Ejemplos de protocolos vector distancias es el RIP que son las siglas de Routing Information Protocol (Protocolo de información de encaminamiento). Es un protocolo de pasarela interior o IGP utilizado por los ruteadores.

Estado del enlace:

Se basa en que un ruteador comunica a los restantes nodos de la red cuáles son sus vecinos y a qué distancias está de ellos. Con la información que un nodo de la red recibe de todos los demás, puede construir un "mapa" de la red y sobre él calcular los caminos óptimos. Un protocolo de estado de enlace es OSPF (Open Shortest Path First) que es un protocolo de pasarela interior o IGP.

3.5.3 ENRUTAMIENTO DEL MINISTERIO

El Ministerio tendrá un enrutamiento estático para enlazar las direcciones públicas con los respectivos servidores y también para las estaciones. La tabla de enrutamiento estático será construida manualmente en los ruteadores y las estaciones como se explica en el capítulo 3. También tendrá un enrutamiento dinámico basado en el protocolo RIP manejado por el Firewall y los Ruteadores públicos ya que la red tendrá múltiples caminos a un mismo destino, lo único que se necesita hacer es ingresar en los ruteadores los comandos apropiados para

que sean capaces de intercambiar información con los ruteadores vecinos y sean capaces de descubrir por si solos la ruta para cada uno de los posibles destinos de la internetwork como se explica en el capítulo 3.

Luego de finalizar el diseño de VLAN´s, definir el direccionamiento IP y las subredes del Ministerio, podemos concluir en el siguiente diseño lógico de la red del Ministerio presentado en la figura 2.5.

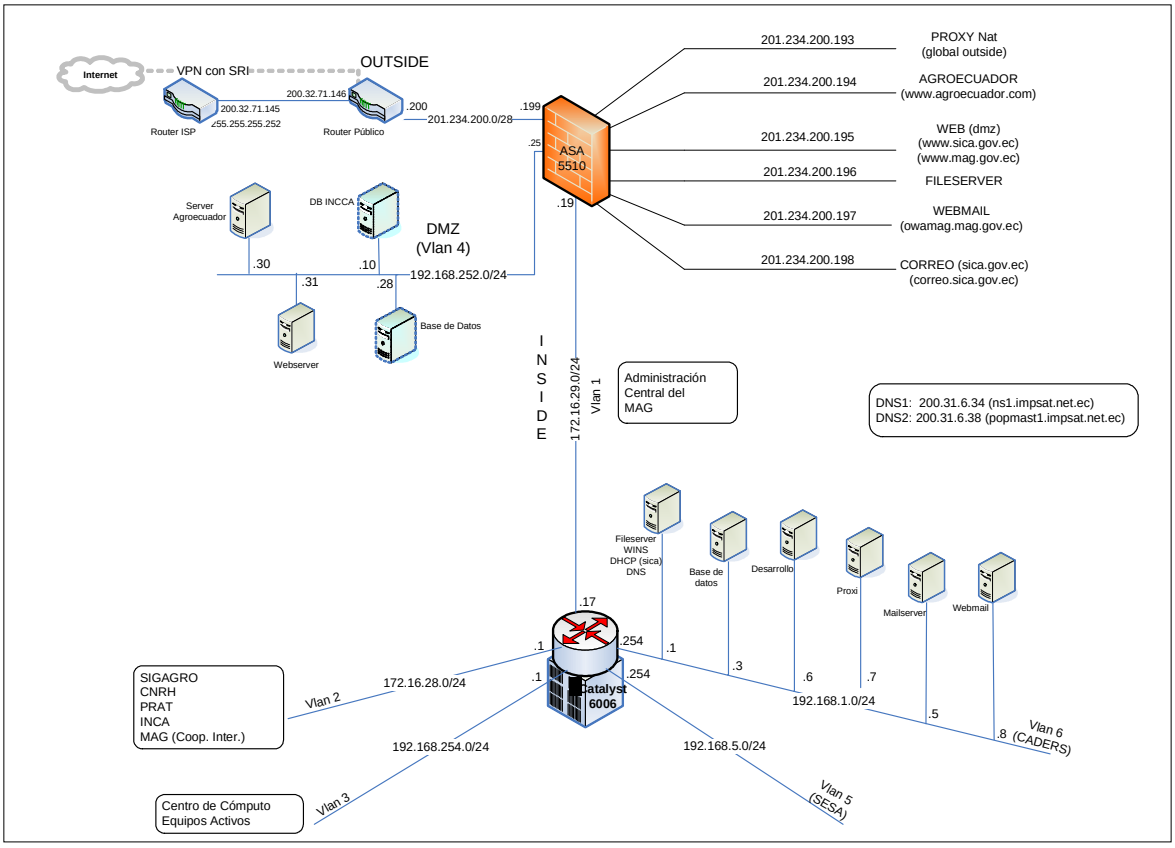


Fig. 2.5 Diagrama lógico del Ministerio

3.6 ALTERNATIVAS DE TECNOLOGÍAS PARA LA IMPLEMENTACIÓN DE LA INFRAESTRUCTURA WAN

Como se mencionó en el capitulo 1, el MAG pretende crear un sistema informático que incluya la interconexión entre la Administración Central, las Subsecretarías Regionales y las Direcciones Provinciales para poder intercambiar información. En esta sección se desarrolla una propuesta de interconexión WAN para satisfacer los requerimientos antes mencionados, pero no se llegará a implementar ya que no es el propósito del presente proyecto.

El sistema que se implante debe ser una solución completa de comunicación de datos que disponga de prestaciones completas LAN y WAN. Para lograr esto se puede pensar en dos escenarios, el uno con infraestructura propia de telecomunicaciones y el otro utilizando Empresas de Servicios Portadores privadas o estatales.

Con el primer escenario, el MAG debe disponer de sus propias líneas de transmisión pero se debe tener muy en cuenta los costos de inversión inicial y mantenimiento que estará en función de su capacidad y tecnología, estos costos son justificables si la frecuencia y volumen de los datos es grande y si la relación costo beneficio es favorable al MAG.

Con el segundo escenario, se debe tener en cuenta que existen diversas tecnologías que se deben acoplar a las necesidades del MAG y estas principalmente son la cantidad y frecuencia de datos a transmitir.

Cuando la frecuencia del intercambio de datos aconseje al MAG mantener una conexión permanente punto a punto, una de las opciones es el alquiler de una línea de transmisión como TDM, la facturación suele ser fija e independiente del volumen de datos transmitidos, le permitiría al MAG disponer de un canal de capacidad fija para su uso exclusivo.

Otra alternativa es el alquiler de circuitos virtuales temporales o permanentes a los operadores de transmisión de datos que ofrecen servicios avanzados de red mediante sus redes de conmutación X.25, Frame-Relay, ATM, etc. Esto permitiría ofrecer al MAG un ancho de banda mínimo para sus conexiones y la posibilidad de aumentar ese ancho de banda si lo necesita. El aprovechamiento de estas líneas de transmisión es mayor ya que al ser compartidas por múltiples usuarios, los periodos de inactividad se reducen al mínimo. En este sentido, Frame Relay se presentan como una de las alternativas más difundidas.

A continuación se analizan en particular dos de estas tecnologías de transporte de información: Clear Channel y Frame Relay, de gran uso en la actualidad, indicando de forma general las características de cada una de ellas, así como los

usos y aplicaciones principales; con la finalidad de seleccionar una de ellas como la tecnología principal de enlace y la otra como tecnología alternativa.

CLEAR CHANNEL (TDM)

Es una tecnología que se basa en la técnica de conmutación de circuitos, orientada a conexión, en donde se puede multiplexar el tráfico en divisiones o slots de tiempo fijos (TDM, Time-Division Multiplexing); la misma que permite enlazar en forma permanente dos puntos predeterminados dentro y fuera del alcance de la red mediante una conexión dedicada y exclusiva.

Por lo general, la compañía (en este caso el MAG) debe tener un puerto disponible DTE (Data Terminal Equipment) que cumpla con las especificaciones técnicas del equipo de comunicaciones entregado por el proveedor. Típicamente la mayoría de los equipos que se usan para recibir los enlaces Clear Channel por parte del cliente son enrutadores o switches de nivel 3.

Entre las características principales de la tecnología TDM se tiene:

- TDM es una tecnología de nivel 1 (físico), es decir, no utiliza ninguno de los protocolos de nivel 2 estándar como PPP (Point to Point Protocol), HDLC (High Level Data Link Control), entre otros; por esta circunstancia, es un canal transparente (Clear Channel) que puede transportar cualquier protocolo, como los mencionados.
- Un enlace Clear Channel ofrece un throughput[10] efectivo casi del 100% ya que no usa ningún tipo de encapsulación de nivel 2, es decir, no hay presentes cabeceras de ningún tipo.
- TDM evita el congestionamiento y retardos variables, es utilizado por el servicio telefónico básico y la RDSI (Red Digital de Servicios Integrados).
- En TDM a los usuarios se les asigna un timeslot[11], y ningún otro cliente puede transmitir en ese timeslot así el propietario no esté transmitiendo. Esto hace que la red no sea muy eficiente.

[10] Cantidad de paquetes que puede procesar y que lleguen a su destino sin perder ninguno.
[11] Espacio de tiempo

- Para el mercado corporativo un enlace Clear Channel comúnmente va desde los 64 Kbit/s hasta los 2048 Kbit/s, en pasos n x 64.
- Clear Channel es ideal para aquellas aplicaciones que necesitan mantener un flujo de información constante, o comunicaciones de gran caudal y calidad por períodos de tiempo prolongados.
- Por sus características especiales Clear Channel sirve de hecho como backbone de alta velocidad para clientes.

Clear Channel es ideal para aplicaciones tales como:

- Aplicaciones Cliente-Servidor.
- Interconexión de redes LAN.
- Tráfico Transaccional.
- Emulación de Terminales.
- Interconexión de redes de voz.
- Interconexión de centros de cómputos.

FRAME RELAY

Frame Relay es un protocolo de conmutación de paquetes, orientado a conexión, que evolucionó de la tecnología X.25 y básicamente difiere de ésta en que usa frames o tramas de longitud variable para el transporte de datos a través de la red. Es usado como una interfaz entre el equipo del usuario, DTE, y el equipo de acceso a la red, DCE. La red a la cual se accede desde este equipo puede ser cualquiera, pública o privada. Desde su introducción en el mercado en 1992, las redes que usan esta tecnología han demostrado su buen performance (prestaciones) unido a una efectividad en costos. Sus características principales son:

- Trabaja en base a circuitos virtuales permanentes (PVC) o conmutados (SVC), en los cuales se establece una ruta entre los extremos al momento de la llamada, funcionando como una línea privada.
- FR puede ser considerado como un protocolo idóneo para el transporte de diferentes protocolos (como SNA, X.25, TCP/IP, DECNET, etc.) de manera

transparente. Esto hace que FR sea compatible con gran parte de los protocolos de alto nivel.

- Los ahorros son significativos al usarse en lugar de líneas dedicadas; además, múltiples usuarios pueden conectarse a una sola línea de acceso, mediante un puerto.
- Equipos terminales como routers pueden ser programados para entender Frame Relay sin necesidad de hacer cambios a nivel de hardware.
- Reduce requerimientos de buffering (almacenamiento) en nodos intermedios y la complejidad de los algoritmos dentro de los mismos, ya que en ellos se elimina la función de corrección de errores y retransmisión. Esto se traduce en menos overhead[12] en los frames y un mejor aprovechamiento del ancho de banda, así como una disminución de los retardos propios de X.25.
- Las velocidades de acceso típicas van desde los 56 Kbps. hasta los 1,544/2,048 Mbps. (T1/E1).
- Es capaz de proveer ancho de banda basado en demanda.
- Es una tecnología basada en estándares internacionales.
- Como tecnología digital, aprovecha la alta potencialidad de las líneas de fibra óptica, menos propensas a fallar.

Actualmente, Frame Relay es usado principalmente para las siguientes aplicaciones:

- Interconexión de LANs: Esto es conectando los routers de dos o más LANs para la transmisión de datos entre ellas.
- Interconexión con redes SNA (Systems Network Architecture): La compatibilidad con interfaces Frame Relay, y la disponibilidad de equipos de acceso Frame Relay que soportan protocolos como SDLC (Shyncronous Data Link Control Protocol), propios de SNA, han hecho posible el trasladar el tráfico de estas redes a redes Frame Relay.
- Soporte de transmisión ideal, en combinación con el protocolo IP, para la explosiva demanda de servicios de los ISP, debido a las altas capacidades

[12] Desperdicio de ancho de banda, causado por la información adicional (de control, de secuencia, etc.) que debe viajar además de los datos.

de conmutación y rápida recuperación de fallas en los enlaces que provee esta tecnología.

- Soporta la transmisión de datos, voz y vídeo.

A la hora de contratar un enlace Frame Relay, hay que considerar que existen dos clases de tráfico:

CIR (Conmited Information Rate o Tasa de Información Comprometida): es la tasa a la cual la red se compromete a transferir datos bajo condiciones normales y sin descartar nada. El CIR (expresado en b.p.s.), es el parámetro sobre el cual se factura.

EIR (Excess Information Rate o Tasa de Información en Exceso): relacionado con el parámetro Be (Excess burst size o ráfaga en exceso), es la cantidad de bits que pueden ser transmitidos en un período de tiempo T por encima del CIR. Este exceso de tráfico, que es proporcionado por defecto y sin costo por la red FR, es definido como de menor prioridad, en condiciones normales será cursado, pero en condiciones de congestión puede ser descartado.

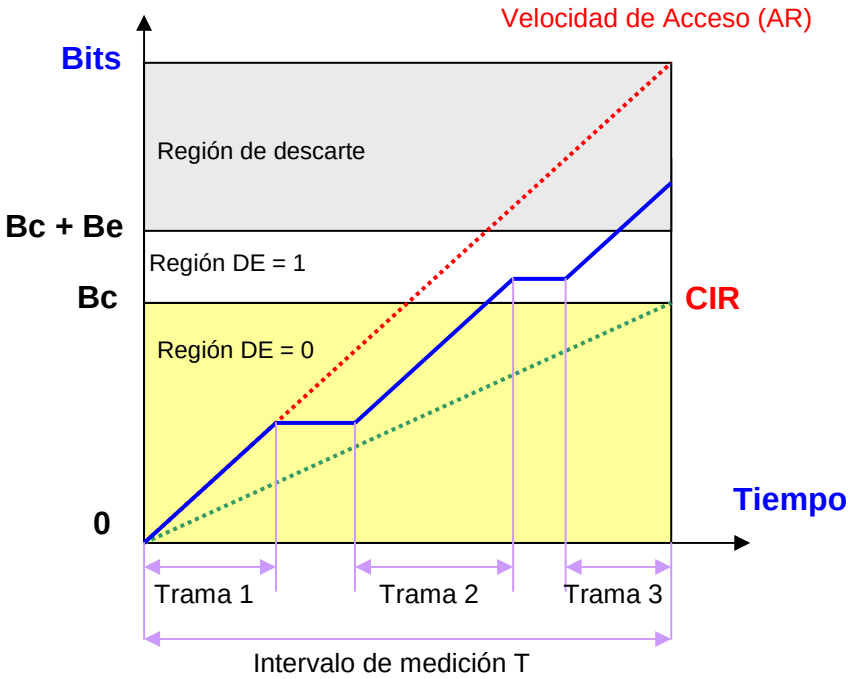


Fig. 2.6 Tarifación Frame Relay

En la figura 2.6 se grafican estos valores y a continuación se dan los conceptos de otros parámetros relacionados.

- Acces Rate (AR).- O Tasa de acceso, es la velocidad de datos del canal de acceso de usuario (expresada en b.p.s.).
- Commited Burst Size (Bc).- O ráfaga comprometida, es el número máximo de bits, durante un intervalo T, que la red se compromete a aceptar tráfico bajo condiciones normales. Bc se define por cada PVC.
- Excess Burst Size (Be).- el número máximo de bits no comprometidos, que la red acepta mas allá del Commited Burst Size, durante un intervalo de tiempo T.
- Measurment Interval (T).- O intervalo de medición, es el intervalo de tiempo durante el cual se permite al usuario enviar el número de bits convenidos (Bc) y el exceso de bits (Be).
- Dado que Bc es la cantidad de bits contratada que puede transmitir el usuario en un tiempo T y el CIR es la velocidad a la que se puede transmitirlos, se tiene que:
- T = Bc/CIR o CIR = Bc/T
- Discard Eligible (DE).- Indicador de elección de descarte de tramas en caso de congestión.

Los proveedores de servicio Fame Relay utiliza los siguientes términos para definir las coberturas de los enlaces:

- LOCAL: Es un enlace de datos proporcionado en el área de una misma ciudad, por ejemplo un enlace Quito-Quito.
- PROVINCIAL: Es un enlace de datos proporcionado en el área de una misma provincia, por ejemplo un enlace Quito-Cayambe.
- REGIONAL: Es un enlace de datos proporcionado en la misma región de Andinatel o Pacifictel, por ejemplo un enlace Ibarra-Ambato.
- NACIONAL: Es un enlace de datos proporcionado en todo el país hacia las otras regiones como Etapa o Pacifictel, por ejemplo un enlace Napo-Cuenca.

- INTERNACIONAL: Es un enlace de datos proporcionado hacia el mundo dando en algunos casos un medio circuito o todo el circuito hacia el punto de destino, por ejemplo: Quito-New York.

En la tabla 2.12 se muestra un resumen de estas tecnologías.

Características	Clear Channel (TDM)	Frame Relay
Conmutación de Circuitos	Si	No
Conmutación de Paquetes	No	Si
Orientado a la conexión	Si	Si
Velocidad (Mbps)	0.064 a 2,048	1,55 a 45
Circuitos Virtuales Permanentes	No	Si
Circuitos Virtuales Conmutados	No	Si
Multiplexación en slots de tiempo	Si	No
Multiplexación estadística	No	Si
Soporte de tráfico de voz	Si	Si
Retardo	Muy Bajo	Bajo

Tabla 2.12 Resumen de las tecnologías analizadas

3.6.1 DEFINICIÓN DE LOS ENLACES WAN CON FRAME RELAY

En base a las consideraciones expuestas anteriormente, y debido a que Frame Relay se encuentra disponible en el país y lo ofrecen varios proveedores de servicios y telecomunicaciones, se opta por utilizar esta tecnología, dejando como alternativa a Clear Channel.

3.6.2 COSTOS

Como es el caso de otros servicios de telecomunicaciones, la tarifación del servicio Frame Relay está sujeta a las correspondientes leyes y reglamentos del Ecuador.

La estimación de los costos por la contratación del servicio público FR, está basada en el Articulo 136 del Reglamento General a la Ley Especial de Telecomunicaciones Reformada referido al Régimen de Tasas y Tarifas, publicado en el Segundo Suplemento del Registro Oficial 194 de 14 Noviembre de 1997, y debidamente autorizada por el Consejo Nacional de Telecomunicaciones (CONATEL), mediante su resolución N° 456-19-CONATEL-

2000 de 5 de Octubre del 2000, publicada en el Registro Oficial N° 201 del 10 de Noviembre del 2000 como se lo presenta en el anexo 5.

2.6.2.1 Estructura Tarifaria del Servicio FR en el Ecuador

En la tabla 2.13 se presentan los costos por inscripción y en la tabla 2.14 se presentan los costos mensuales por el servicio Frame Relay de acuerdo a la cobertura vigentes en el Ecuador.

- Derecho de Inscripción

Tipo de Enlace	LOCAL	PROVINCIAL	REGIONAL	NACIONAL
INSCRIPCIÓN (USD)	250	400	400	500

Tabla 2.13 Derecho de inscripción para circuitos Frame Relay

Por cada extremo se deberá añadir el valor de acometida.

- Renta Mensual del Servicio

VELOCIDAD EN Kbps		LOCAL	PROVINCIAL	REGIONAL	NACIONAL
CIR	MBR[13]	MENSUAL (USD)	MENSUAL (USD)	MENSUAL (USD)	MENSUAL (USD)
768	1024	950,00	1.995,00	2.800,00	4.275,00
512	768	800,00	1.680,00	2.360,00	3.600,00
384	512	600,00	1.260,00	1.770,00	2.700,00
256	384	450,00	945,00	1.330,00	2.025,00
128	256	250,00	525,00	740,00	1.125,00
64	128	140,00	294,00	410,00	630,00
32	128	126,00	264,60	365,00	555,00
32	64	118,00	247,80	340,00	520,00
19,2	64	112,00	235,20	325,00	495,00
9,6	64	103,60	217,56	300,00	456,00
19,2	32	103,60	217,56	300,00	456,00
9,6	32	94,00	197,40	270,00	410,00
9,6	19,2	76,00	159,60	220,00	335,00
Circuito virtual		15,60	45,00	45,00	70,00

Tabla 2.14 Tarifas mensuales para circuitos Frame Relay[14]

Estos precios incluyen el presupuesto especial (valor del arrendamiento y uso de equipos terminales).

[13] MBR: Maximum Bit Rate
[14] Registro Oficial N° 201 del 10 de noviembre del 2000

Según estas tablas, los costos de inscripción y mensualidades para las Subsecretarías y Direcciones Provinciales del MAG se presentan de las tablas 2.15 a la 1.18.

Nodo 1	Nodo 2	**TIPO DE ENLACE**	**INSCRIPCIÓN (USD$)**
Guayas	MAG	Nacional	500
Manabí	MAG	Nacional	500
Chimborazo	MAG	Regional	400
Napo	MAG	Regional	400
		Total	1,800

Tabla 2.15 Derecho de inscripción para las Subsecretarías

Nodo 1	**Nodo 2**	**TIPO DE ENLACE**	**INSCRIPCIÓN (USD$)**
Esmeraldas	Manabí	Nacional	500
Los Ríos	Guayas	Regional	400
El Oro	Guayas	Regional	400
Galápagos	Guayas	Regional	400
Carchi	Chimborazo	Regional	400
Imbabura	Chimborazo	Regional	400
Pichincha	Chimborazo	Regional	400
Cotopaxi	Chimborazo	Regional	400
Tungurahua	Chimborazo	Regional	400
Bolívar	Chimborazo	Regional	400
Cañar	Chimborazo	Nacional	500
Azuay	Chimborazo	Nacional	500
Loja	Chimborazo	Nacional	500
Pastazav	Napo	Regional	400
Morona Santiago	Napo	Nacional	500
Zamora Chinchipe	Napo	Nacional	500
Sucumbíos	Napo	Regional	400
Orellana	Napo	Regional	400
		Total	7,800

Tabla 2.16 Derecho de inscripción para las Direcciones Provinciales

Nodo 1	Nodo 2	Tipo de enlace	FRAME RELAY		
			Velocidad (Kbps)		Mensual (USD$)
			CIR	MBR	
Guayas	MAG	Nacional	64	128	630
Manabí	MAG	Nacional	128	256	1,125
Chimborazo	MAG	Regional	64	128	410
Napo	MAG	Regional	64	128	410
		Total ($)			2,575

Tabla 2.17 Tarifa mensual FR para las Subsecretarías

Nodo 1	Nodo 2	Tipo de enlace	FRAME RELAY		
			Velocidad (Kbps)		Mensual (USD$)
			CIR	MBR	
Esmeraldas	Manabí	Nacional	64	128	630
Los Ríos	Guayas	Regional	64	128	410
El Oro	Guayas	Regional	64	128	410
Galápagos	Guayas	Regional	64	128	410
Carchi	Chimborazo	Regional	64	128	410
Imbabura	Chimborazo	Regional	64	128	410
Pichincha	Chimborazo	Regional	128	256	740
Cotopaxi	Chimborazo	Regional	64	128	410
Tungurahua	Chimborazo	Regional	64	128	410
Bolívar	Chimborazo	Regional	64	128	410
Cañar	Chimborazo	Nacional	64	128	630
Azuay	Chimborazo	Nacional	64	128	630
Loja	Chimborazo	Nacional	64	128	630
Pastazav	Napo	Regional	64	128	410
Morona Santiago	Napo	Nacional	64	128	630
Zamora Chinchipe	Napo	Nacional	64	128	630
Sucumbíos	Napo	Regional	64	128	410
Orellana	Napo	Regional	64	128	410
		Total ($)			8,540

Tabla 2.18 Tarifa mensual FR para las Direcciones Provinciales

A continuación en la figura 2.7 se presenta el diagrama lógico de la interconexión entre la Administración Central del MAG y las Subsecretarías Regionales, y en las figuras 2.8 y 2.9 se muestran las ubicaciones de estas Subsecretaría como también las coberturas por regiones que rigen en el país.

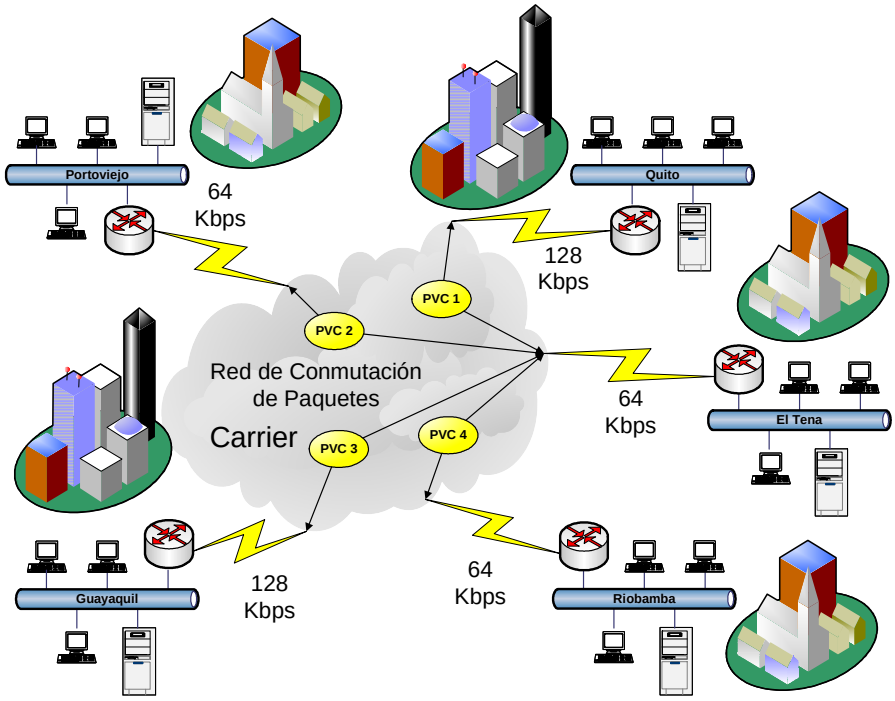


Fig. 2.7 Diagrama lógico de la interconexión entre Subsecretarías.

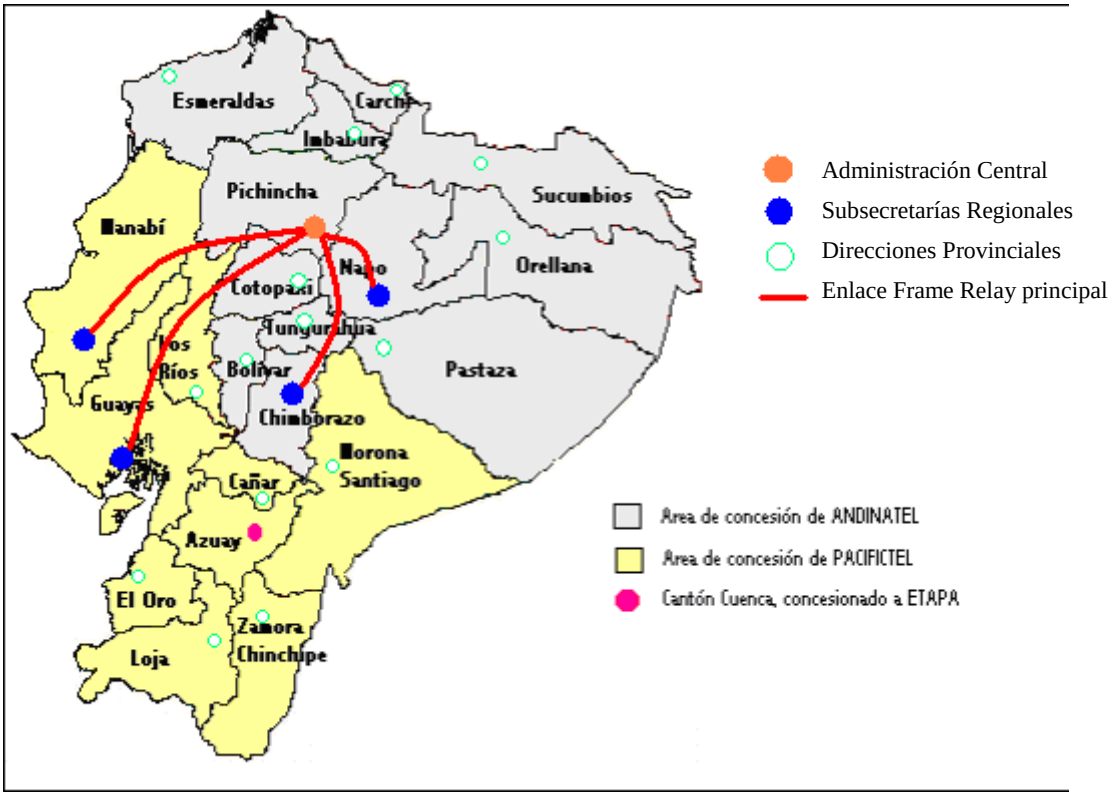


Fig. 2.8 Distribución física de las Subsecretarías Regionales.

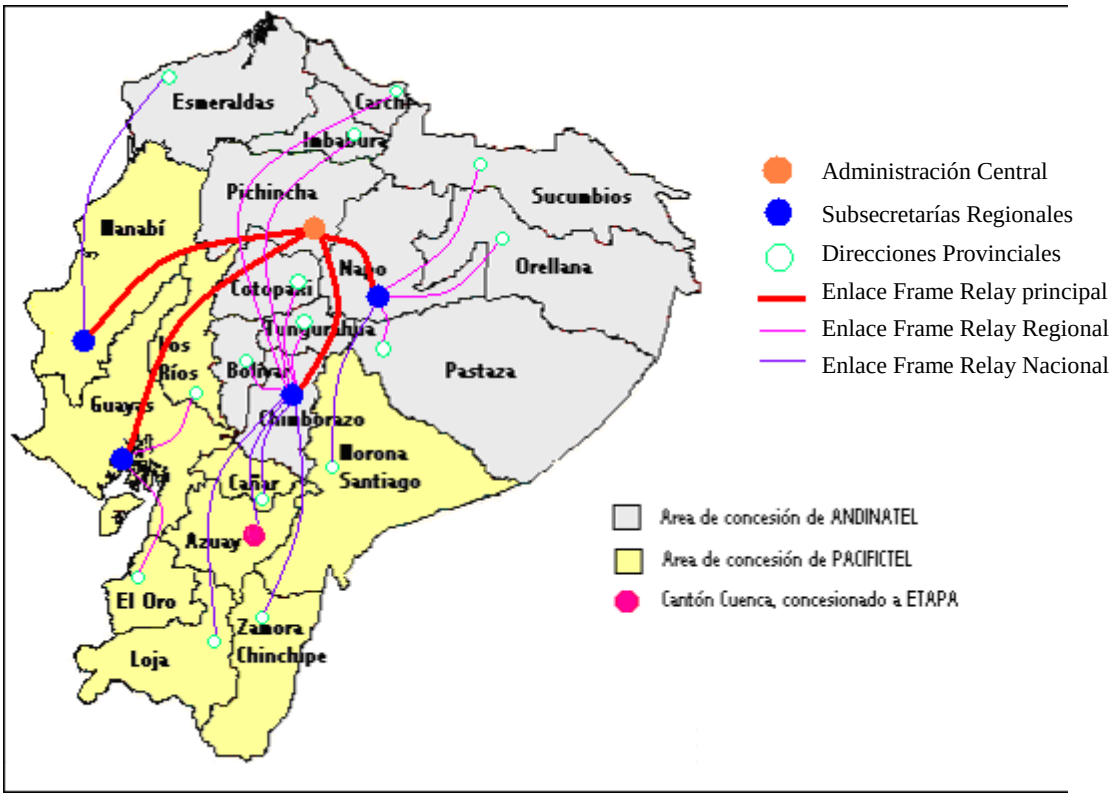


Fig. 2.9 Distribución física de las Direcciones Provinciales.

3.6.3 EQUIPOS DE INTERCONEXIÓN

Para interconectar redes Frame Relay como las que se propone, es necesario dispositivos que entiendan los protocolos de interfase, estos equipos son los FRAD[15] que ofrecen fácil mapeo de los DCLI[16] y pueden ejecutar limitadas funciones de ruteo. Se puede usar también CSU/DSU[17] que básicamente son equipos que conecta el ruteador de una red LAN con una línea digital.

Estos equipos son proporcionados por los proveedores del servicio y su arrendamiento está incluido en las tarifas mensuales pero para tener una idea de sus costos y que equipos son, mencionaremos dos de ellos.

[15] Frame Relay Access Devices
[16] Data Link Connection Identifier
[17] Channel Service Unit/Data Service Unit

La línea de productos Loop-E1500 CSU/DSU provee una solución económica para este tipo de redes. El puerto DTE puede operar desde 56 kbps. hasta 2048 kbps. soporta control local y diagnóstico utilizando el teclado y pantalla LCD o el puerto RS-232. Mediante SNMP o Telnet, el usuario puede controlar y diagnosticar el equipo desde cualquier parte, su costo es de USD$ 1,120.00.

Otro equipo muy utilizado es el ADTRAN EXPRESS 5210 FRAD 56/64 DSU/CSU que es un manejador de tráfico de voz y datos sobre redes Frame Relay, su costo es de USD$ 1,295.00.

En el anexo 3 se muestran las características técnicas de estos equipos.

CAPITULO 3

IMPLEMENTACIÓN DE LA RED DE CAMPUS EN TRES CAPAS DEL MAG

3.1 IMPLEMENTACIÓN DE EQUIPOS

Esta implementación está financiado por el Banco Mundial y esta institución dicta ciertas exigencias de carácter tecnológico para aprobar el crédito, entre estas exigencias están las marcas y procedencias de los equipos y materiales a utilizarse en el proyecto.

Entre las marcas para equipos de computación están DELL, Compaq y HP, la marca para equipos de comunicación es Cisco y los elementos para cableado estructurado es Alcatel.

Antes de hacer la implementación con equipos Cisco, se hará un análisis comparativo con otras marcas para ver su relación de costos y que se resume en el siguiente cuadro:

Fabricante	Modelo	Capas SAFE	Fast Eth	Giga Eth	Costo USD$
Cisco	WS C2950-24	Capa Acceso	24	2	1.200,00
Cisco	WS C3548-XL	Capa Distribución	48	2	2.400,00
Cisco	Catalyst 6006	Capa Core	Hasta 120	Hasta 40	9.200,00
3Com	3C16475-US	Capa Acceso	24	2	650,00
3Com	3CR17501-91	Capa Distribución	48	2	1.450,00
3Com	3C16894 –4 Slots	Capa Core	Hasta 144	Hasta 148	3.200,00
D-Link	DES-3828DC	Capa Acceso	24	4	700,00
D-Link	DXS-3350SR	Capa Distribución	-	48	1.500,00
D-Link	DES-6500 8 Slots	Capa Core	Hasta 192	Hasta 96	2.950,00

Tabla 3.1 Análisis comparativo con otras marcas

Para la implementación de los equipos de la red del Ministerio, los vamos a dividir jerárquicamente como en el diseño.

3.1.1 CAPA DE ACCESO

Los switches Cisco para capa de acceso son los de la serie Catalyst como los 1900, 2820, 2950, 4000 y 5000, la tabla 3.2 nos indica algunas características de estos switches.

Serie Catalyst	Tipo	Capas OSI	Ethernet	Fast Eth	Giga Eth	Tamaño empresarial
1900	Config. Fija	Capa 2	12 o 24	2	0	Pequeño o mediano
2820	Fija+spot exp. Modul.	Capa 2	24	2	0	Pequeño o mediano
2950	Config. fija	Capa 2	0	12 o 24	0 o 2	Pequeño o mediano
4000	Modular	Capa 2 y 3	Config. 240	Config. 240	Config 240	Según opciones
5000	Modular	Capa 2 y 3	Config 528	Config 266	Config 38	Según opciones

Tabla 3.2 Características generales de Switchs Capa de Acceso

El switch que se ha escogido como base para la capa de acceso es el Cisco Catalyst 2950 de 24 o 48 puertos (WS C2950-24, WS C2950-48) por su facilidad de administración y por que ya disponen de algunos de estos, sus características se detallan en el anexo 3.

También en la capa de acceso se instalarán otros modelos de Switches Cisco y Switch 3Com y que se los utiliza por que el Ministerio dispone de estos, los modelos son los siguientes:

- Switch Catalyst 2924-24
- Switch Catalyst 2924C-24
- Switch 3Com 3C16475
- Switch 3Com 3CR17501-91

En la tabla 3.3 se detallan los switches de capa de acceso que se necesitan por cada IDF según el diseño del capitulo anterior y del MDF ya que también ahí se concentrarán usuarios.

	SW Nuevos		SW Existentes			
# IDF	C2950-48	C2950-24	C2924-24	C2924C	3C16475	3CR17501
1			1			
2						1
3		1				
4		1				
5	1	1			1	
6			3			
7					1	
8		2			1	
9				1		
10					1	
11		1	1			
12					1	
MDF	1	1	1		2	

Tabla 3.3 Número de Switchs en la Capa de Acceso

Teniendo un total de Switchs como se detalla en la tabla 3.4.

SW Nuevos		SW existentes			
C2950-48	C2950-24	C2924	C2924C	3C16475	3CR17501
2	7	6	1	7	1

Tabla 3.4 Total de Switchs en la capa de Acceso

3.1.2 CAPA DE DISTRIBUCIÓN

Los Switches de la capa de distribución son los puntos de totalización de múltiples Switches de la capa de acceso, deben tener un alto rendimiento ya que es el punto en el que se encuentra delimitado el dominio de Broadcast, la capa de distribución combina el tráfico VLAN.

Los Switches que recomienda Cisco para capa de distribución son:

- Catalist 3500
- Catalist 2926G
- Familia Catalist 5000
- Familia Catalist 6000

El Switch que se utilizará en esta capa de distribución es el Catalyst 3548 principalmente por el costo, por su densidad de puertos y por su fácil administración, sus características se detallan en el anexo 3.

Debido a que se dispone de el Switch 3Com 3CR17501 se lo utiliza en la capa de distribución y que por sus características físicas no se tendrá ningún problema en el diseño, en la tabla 3.5 se detallan los switches de capa de distribución que se necesitan por cada IDF y MDF según el diseño del capitulo anterior.

# de IDF	WS-C3548-XL-EN	3CR17501
1	2	
2		1
3	1	
6	1	
8	1	
13	1	
MDF	1	

Tabla 3.5 Número de Switchs en la Capa de Distribución

No se mencionan el resto de IDF´s por que en estos no se instalan Switchs de distribución.

3.1.3 CAPA NÚCLEO

La capa núcleo es el backbone de la red conmutada de campus, los Switches de esta capa pueden hacer uso de una serie de tecnologías de capa 2, la capa núcleo puede ser enrutada o de capa 3.

Los Switches de la capa núcleo están diseñados para ofrecer funcionalidad de capa 3 eficiente, los Switches que recomienda Cisco para capa núcleo son:

- Serie catalyst 6000
- Serie catalyst 8500
- Serie IGX 8400
- Ligtstream 1010

El Switch que se utilizará en esta capa núcleo es el Catalyst 6006 principalmente por el costo, por su densidad de puertos, por su velocidad de BackPlane de 32-

Gbps, por su fácil administración y sus capacidades de redundancia como la tarjeta de supervisión, la fuente de poder y las interfaces.

El Switch Catalyst 6006 tiene seis slots horizontales. El slot 1 es reservado para la tarjeta de supervisión la cual provee administración local y remota, y múltiples interfaces uplink gigabit.

El slot 2 puede contener otra tarjeta de supervisión la cual puede actuar como respaldo de la primera si falla, si no se requiere esta segunda tarjeta, el slot 2 está disponible para un módulo switching.

El Switch Catalyst 6006 puede soportar lo siguiente:

- Una tarjeta de supervisión con dos puertos uplink Gigabit Ethernet y una tarjeta redundante opcional.
- Un backplane con un ancho de banda de 32 Gbps.
- Ventiladores redundantes Hot-Swappables.
- Hasta cinco módulos adicionales Hot-Swappables.

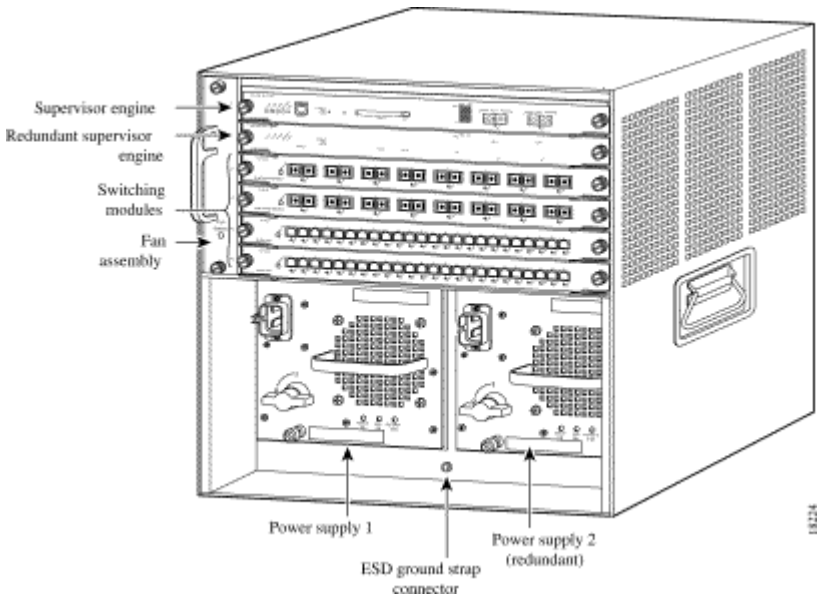


Fig. 3.1 Switch Catalyst 6006

En el anexo 3 se describen las características de hardware del Switch Catalyst 6006.

Solo utilizaremos un Switch WS-C6006 en el MDF del piso 6.

3.1.4 SEGURIDAD

Cisco sacó la nueva serie de Firewalls ASA5500, esta nueva solución combina una de las mejores creaciones en seguridad y servicio VPN con la innovadora arquitectura "Cisco Adaptative Identification and Migration (AIM)".

Diseñado con el componente clave: la solución Cisco "self-defending network", el mismo que facilita una respuesta proactiva ante amenazas, deteniendo los ataques antes de que los propaguen por la red, controlando la actividad de la red y el tráfico, permitiendo la creación de VPN para la conectividad flexible.

El Cisco ASA 5500 series, es una solución efectiva y eficiente, protegiendo las redes y a la vez facilitando el retorno de la inversión.

Esta serie incluye los modelos ASA 5510, ASA 5520 y ASA 5540, tres soluciones de seguridad de alto rendimiento que integran las últimas tecnologías de la serie Cisco PIX500, IPS 4200 y CVPN3000. Por la combinación de estas tecnologías en uno, el ASA 5500 series es una solución compacta y mejorada que permite proteger de ataques a las redes.

Para la seguridad del MAG se ha escogido el Cisco ASA 5510 destinado a PYMES y empresas mayores con conexiones remotas ya que es una solución fácil de instalar, con un coste efectivo. Puede ser fácilmente gestionado y monitorizado con una aplicación basada en Web.

Este modelo incluye funciones de Firewall de alto rendimiento y servicio VPN, integra 3 puertos FE y prevención de Intrusión, a través del Módulo de Servicios de Seguridad (SSM) convirtiéndolo en una elección excelente en sitios en que requieran una solución de seguridad efectiva, extensible con opción DMZ como es nuestro caso.

Fig. 3.2 Cisco ASA 5510

En el anexo 3 se describen las características del firewall Cisco ASA 5510.

La figura 3.3 muestra un esquema general de cómo quedará la red del Ministerio

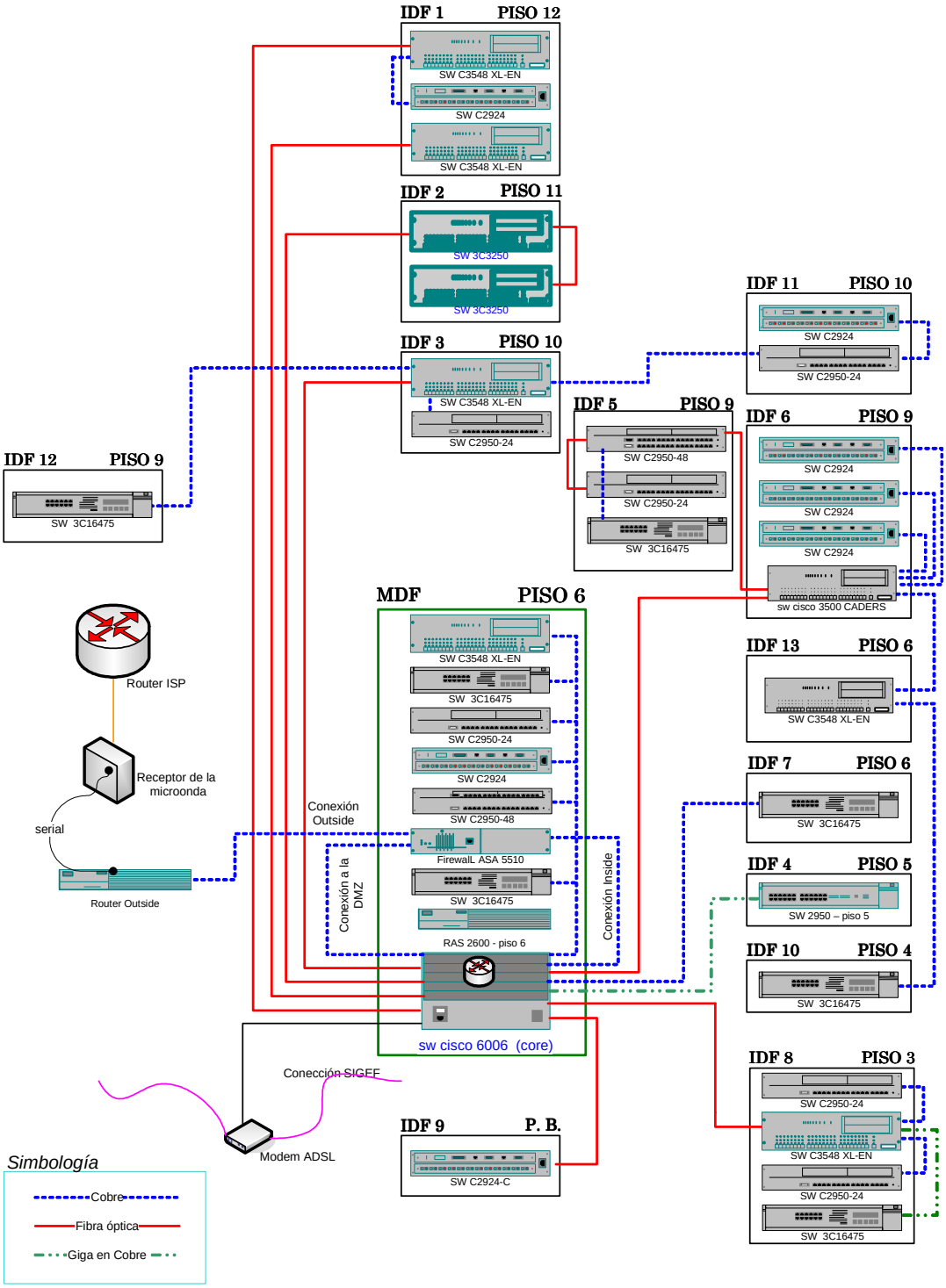


Fig. 3.3 Distribución de equipos en el MAG.

3.2 DISTRIBUCIÓN DE CABLEADO Y EQUIPOS

3.2.1 CONSIDERACIONES DE CONSTRUCCIÓN PARA EL CABLEADO ESTRUCTURADO

La administración del MAG y sus dependencias tienen un sistema de cableado estructurado, lo que permite las comunicaciones de manera integral.

Este sistema de cableado estructurado cumple con las normas internacionales que se mencionan a continuación en la tabla 3.6:

NORMA	ESPECIFICACIÓN
ANSI/TIA/EIA-568-B	Estándares de cableado para telecomunicaciones en edificios comerciales.
ANSI/TIA/EIA-570	Estándar de alambrado de telecomunicaciones Residencial y comercial liviano.
EIA/TIA-569	Estándares para instalación y dimensionamiento de cableado estructurado en edificios comerciales.
ANSI/TIA/EIA-607	Requerimientos para telecomunicaciones de puesta a tierra y puenteado de edificios comerciales.
EIA/TIA-606	Estándares de administración para la infraestructura de telecomunicaciones
ISO 11801	Estándares de cableado para telecomunicaciones en edificios comerciales.

Tabla 3.6 Normas Internacionales para Cableado Estructurado

El sistema de cableado estructurado del MAG y sus dependencias contempla los siguientes subsistemas:

a) Área de Trabajo.
b) Cableado Horizontal.
c) Closets de telecomunicaciones.
d) Cableado vertical.
e) Cuarto de equipos de telecomunicaciones principal.

a) **Subsistema área de trabajo**

Comprende los elementos de cableado estructurado (cables, conectores, adaptadores, etc.) que permiten la conexión de los equipos terminales (estaciones de trabajo) con las salidas de información.

Para la determinación de los puntos de red, se utilizaron los planos arquitectónicos de cada uno de los pisos y se los ubicó de acuerdo a cada dependencia y de acuerdo a la función que desempeñan cada usuario, además esta ubicación se ratificó mediante visitas a todas las dependencias del MAG.

En la tabla 3.7 se presenta de manera resumida el número de puntos determinados para cada IDF.

IDF	PUNTOS EXISTENTES	PUNTOS DETERMINADOS	PUNTOS ADICIONALES
1	67	90	23
2	64	90	26
3	65	65	0
4	20	20	0
5	79	80	1
6	75	90	15
7	23	23	0
8	65	85	20
9	14	20	6
10	21	21	0
11	21	30	9
12	21	21	0
13	20	20	0
MDF	135	160	25

Tabla 3.7 Número de puntos por cada IDF

Los cables de conexión (patch cord) entre la toma y el equipo terminal son preconectarizados (construidos) en fábrica con conectores tipo RJ-45 a los dos lados, de 3 metros de longitud máxima. Cumplen con los siguientes requerimientos de las normas para categoría 5e de la ISO/IEC IS 11801, EN 50173 Y EIA/TIA 568B:

- El patch cord de cobre es multifilar (no sólido) UTP de 4 pares con un conector de 8 posiciones y 8 contactos macho en cada extremo.

- La cantidad de Patch Cord que se requieren para los puntos adicionales es uno por cada punto, por lo que se requieren 125 Patch Cord de 3 metros.

b) **Subsistema cableado horizontal**

Este subsistema comprende los elementos que permiten la conexión de las áreas de trabajo con el respectivo closet de telecomunicaciones, se considera la topología física y los aspectos relacionados con el medio de transmisión como tipo de cable, cálculo de la distancia y método de distribución.

La topología física como se mencionó en el diseño es estrella extendida ya que cada salida se conecta a los IDF´s. El cable horizontal es tipo UTP categoría 5e calibre 24 (24 AWG) de 4 pares compuesto por conductores sólidos, trenzados conforme a los estándares ISO/EC IS 11801, EN 50173, EN 50167, EN 50168, EIA/TIA 568B, certificado para transmisión de hasta 100 MHz. de frecuencia, impedancia característica 100 Ohmios, chaqueta de PVC retardante al fuego de acuerdo a la norma IEC 332-1.

La longitud individual de cada corrida de cable desde el closet de telecomunicaciones hasta las tomas no excederá en ningún caso los 90 metros.

Luego de ubicar los puntos de red adicionales en los planos, se procedió a determinar la ruta que seguirá el cableado dentro de cada piso.

El cálculo del número de rollos de cable para el cableado horizontal se realizó utilizando el método propuesto por Alcatel, el cual consiste en:

Cálculo de la longitud promedio por punto.

Long. Media = (Long. Máx + Long. Min.)/2 + 5 [metros]

Se le aumenta 5 metros para cubrir la subida o bajada a la placa o al IDF.

Cálculo del número de corridas por rollo.

corridas por rollo = Long. Cable por rollo / Long. Media

A este valor se le aproxima por debajo debido a que el último segmento en el rollo es un sobrante no utilizable, además la longitud del cable por rollo es una constante de 305 metros. (1000 pies).

Cálculo de la cantidad de rollos de cable.

de rollos = # de salidas / # corridas por rollo

A este valor se lo aproxima por arriba para obtener un valor entero de números de rollos.

Los resultados del cálculo de longitud promedio y del número de rollos necesarios por piso en cada IDF se muestran en la tabla 3.8 que está a continuación.

IDF	PUNTOS ADICIONALES	LONGITUD MEDIA	CORRIDAS POR ROLLO	CANTIDAD DE ROLLOS
1	23	28	10	3
2	26	28	10	3
3	0			
4	0			
5	1	19	16	0
6	15	25	12	2
7	0			
8	20	29	10	2
9	6	22	13	1
10	0			
11	9	23	13	1
12	0			
13	0			
MDF	25	27	11	3

Tabla 3.8 Cantidad de rollos para los puntos adicionales

Placas de pared

Las placas de pared cumplirán a cabalidad y simultáneamente con las características detalladas a continuación:

- Las placas de pared contendrán de fábrica, una ranura para insertar la etiqueta de identificación correspondiente.
- La placa albergará los conectores modulares. El módulo que soporta el conector será desmontable de la placa para acceder el cable horizontal.
- La placa podrá tener una inclinación para evitar que cualquier doblamiento del cable UTP de 4 pares sobrepase el radio mínimo de curvatura de 4 veces el diámetro externo del cable.

La conexión entre el cable UTP de 4 pares y el conector será mediante contactos de desplazamiento de aislante IDC (insulation displacement conectors).

El conector soportará los esquemas T568A y T568B de conexión.

La cantidad de Placas de Pared que se requieren para los puntos adicionales es una por cada punto, por lo que se requieren 148 Placas de Pared.

c) **Subsistema closet de telecomunicaciones**

El subsistema closet de telecomunicaciones (IDF) está constituido por los elementos de Interconexión entre el subsistema cableado vertical (backbone) y el subsistema cableado horizontal, se los ubicará en su mayoría en cuartos pequeños a un lado de las gradas y contarán con iluminación y ventilación adecuada al igual que con instalación de tierra, fuente de energía ininterrumpida y seguridad física. En los planos del Anexo 1 se presenta la ubicación de cada uno de los closets de telecomunicaciones (IDF´s).

Los closets de telecomunicaciones cumplirán las normas y requerimientos del EIA/TIA-569, serán racks cerrados de pared de 19 pulgadas de ancho para instalación de los elementos componentes del cableado como Patch Panels, Patch Cord y la electrónica necesaria.

Los Patch Cord categoría 5e formado por cable UTP (Unshielded Twisted Pair) flexible no sólido, preconectorizado de fábrica con conectores tipo RJ-45 a los dos lados de máximo 1,5 metros de longitud, para conexión de los equipos de datos con el cableado horizontal. Deberá cumplir con los requerimientos de las normas para categoría 5e de la TIA/EIA-568B.

Los organizadores horizontales de 19 pulgadas de ancho metálicos, para organización de Path Cords.

Estos racks ya se encuentran instalados y funcionando pero para ver si soportan el crecimiento los vamos a dimensionar nuevamente.

A continuación se realizará el dimensionamiento del rack para el IDF 1 del piso 12 perteneciente a la administración del MAG, el mismo que nos servirá como modelo para los demás.

El diseño del cableado horizontal para el IDF 1 presenta 90 puntos de datos, para lo cual se necesita 2 patch panel de 48 puertos los mismos que representan 3 unidades de rack cada uno (3 UR), cada unidad de rack representa a 1,75 pulgadas, se tendrán 4 organizadores de 1UR, se instalarán 3 Switches de 1UR, por lo que se necesita un total de 13UR, manteniendo un 40% de holgura se debe disponer de un rack de por lo menos 19UR, El rack que se dispone en el piso 12 es de 24UR por lo que nos calza perfectamente.

El dimensionamiento de todos los rack del Ministerio se resume en la tabla 3.9.

IDF	Unidades de rack necesarias	Tamaño del rack actual (UR)
1	19	24
2	19	24
3	16	24
4	8	18
5	19	24
6	19	24
7	9	12
8	22	42
9	4	12
10	4	12
11	5	12
12	4	12
13	4	12
MDF	40	42

Tabla 3.9 Dimensionamiento de racks para el Ministerio

La tabla 3.10 muestra la cantidad de elementos pasivos por cada IDF según el diseño anterior.

IDF	Patch Panel			Patch Cord	Patch Guide
	12 puertos	24 puertos	48 puertos		
1			2	90	4
2			2	90	4
3		1	1	65	3
4		1		20	1
5			2	80	4
6			2	90	4
7		1		23	1
8			2	85	4
9		1		20	1
10		1		21	1
11		2		30	2
12		1		21	1
13		1		20	1
MDF	1	7		160	8

Tabla 3.10 Cantidad de elementos en los IDF´s

d) **Subsistema Cableado Vertical**

Este subsistema estará constituido por los cables de fibra óptica o cobre que unirán el closet de telecomunicaciones con el cuarto de telecomunicaciones.

El Ministerio de Agricultura y Ganadería utilizará fibra óptica en la mayoría de enlaces de los IDF´s y el MDF y solo en algunos enlaces se utilizará cable FTP como lo muestra la figura 2.3 del capitulo 2.

La composición básica de un cable de fibra óptica consta de un núcleo o Core (n1), una cubierta o Cladding (n2) y un revestimiento externo protector. El núcleo es el conductor de la señal luminosa, su atenuación es despreciable y tiene mayor índice de refracción que la cubierta (n1>n2). La señal es conducida por el interior de este núcleo fibroso, sin poder escapar de él debido a las reflexiones internas que se producen.

Por el modo de propagación de la luz existen dos clases de fibra óptica para la transmisión de datos:

Fibra Monomodo: Esta fibra tiene un core muy delgado que es el único camino para la propagación de la luz, usa un LASER como fuente de luz, puede cubrir

hasta 3Km (25Km en telefonía), el revestimiento es de color amarillo, permite una transmisión de señales con ancho de banda hasta 100 GHz. y sus dimensiones típicas son:

núcleo (υm)	cubierta (υm)	revestimiento (υm)
8.3 - 10	125	250 / 900

Fibra Multimodo: Proporciona varios caminos de propagación de la luz, puede alcanzar una distancia de 2Km, usa un LED como fuente de luz, su revestimiento es de color anaranjado y cuyas dimensiones típicas son:

núcleo (υm)	cubierta (υm)	revestimiento (υm)
50	125	250 / 900
62.5	125	250 / 900
100	140	

La fibra multimodo a su vez se subdivide en:

- Fibra Multimodo de índice gradual (graded-index): El core está compuesto de varias capas, la forma de propagación de la luz es senosoidal, tiene un ancho de banda de hasta 500 MHz.

- Fibra Multimodo de índice escalonado (steep-index): La luz incide con un cierto ángulo al medio de transmisión, tiene un ancho de banda de 35 MHz.

Por la fabricación también se pueden encontrar de:

- Tight Buffered: configuración apretada, se usa para interiores y exteriores, chaqueta “tight buffer” protege cada fibra aumentando el diámetro 900 um y es de fácil conectorización.

- Loose Tube: Configuración Suelta, se usa para exteriores, puede requerir un “breakout kit” para conectorizar

Por el tipo de material existen de Core y Clanding de Plástico, Core de Vidrio y Clanding de Plástico y Core y Clanding de Vidrio.

Entre las ventajas tenemos que la fibra óptica es inmune al ruido y las interferencias, las fibras no pierden luz, por lo que la transmisión es también segura y no puede ser perturbada, carencia de señales eléctricas en la fibra, presenta dimensiones más reducidas que los medios preexistentes, el peso del cable de fibras ópticas es muy inferior al de los cables metálicos, la materia prima para fabricarla es abundante en la naturaleza, compatibilidad con la tecnología digital.

La fibra óptica que se instalará en el ministerio será del tipo multimodo de 62.5/125 micrones de 6 hilos con chaqueta de PVC.

Documentación técnica

Se entregará un plano de cada instalación en AUTOCAD impreso y digital, indicando:

- Ubicación de cada puesto de trabajo y su nombre asignado
- Ruta de canalizaciones
- Ubicación del Closet de Telecomunicaciones

Se entregará un reporte por cada toma de telecomunicaciones donde se indica los siguientes datos de cada enlace:

- Longitud
- Atenuación
- NEXT (tomar el peor par como el valor del enlace)
- Chequeo de: continuidad, cortos, abiertos, inversión y transposición de pares

Adicionalmente se indicará las condiciones generales en las cuales se realizó la medición.

- Nivel máximo de ruido aleatorio
- Next residual
- Balance de la señal de salida
- Rechazo en modo común
- Precisión dinámica y pérdida de retorno

Las pruebas se realizarán con un probador marca Fluke DSP-4100 que permite una inyección doble de señales en forma simultánea, es decir, realizará mediciones en ambos sentidos, de extremo a extremo, en cada segmento de cable, los resultados de un punto de cada red se los muestra en el anexo 2.

e) **Cuarto de equipos de telecomunicaciones principal**

Como ya mencionamos en el diseño del capítulo 2, el cuarto de equipos del ministerio se ubicará en el piso 6 y es donde se alojarán los servidores y el MDF

La altura mínima recomendada del cielo raso es de 2.6 metros, los ductos utilizados para acceder el cuarto de telecomunicaciones son tres de 100 milímetros (4 pulgadas) para la distribución del cable del backbone. La puerta de acceso debe ser de apertura completa, con llave y de al menos 91 centímetros de ancho y 2 metros de alto. Se debe evitar el polvo y la electricidad estática utilizando piso de concreto, terrazo, loza o similar (no utilizar alfombra).

Este cuarto como tiene equipos electrónicos la temperatura debe mantenerse continuamente (24 horas al día, 365 días al año) entre 18 y 24 grados centígrados. La humedad relativa debe mantenerse entre 30% y 55.

Se pusieron tomacorrientes suficientes para alimentar los dispositivos instalados en los racks, los tomacorrientes son dobles de 110V C.A. dedicados de tres hilos en circuitos separados de 15 a 20 amperios. La alimentación específica de los dispositivos electrónicos se los hace con UPS y regletas.

El cuarto de telecomunicaciones cuenta con una barra de puesta a tierra que a su vez está conectada mediante un cable 6 AWG con aislamiento verde al sistema de puesta a tierra de telecomunicaciones según las especificaciones de ANSI/TIA/EIA-607.

Los racks deben de contar con al menos 82 cm. de espacio de trabajo libre alrededor (al frente y detrás) de los equipos y paneles de telecomunicaciones. La distancia de 82 cm. se debe medir a partir de la superficie más salida del rack.

Se recomienda dejar un espacio libre de 30 cm. en las esquinas.

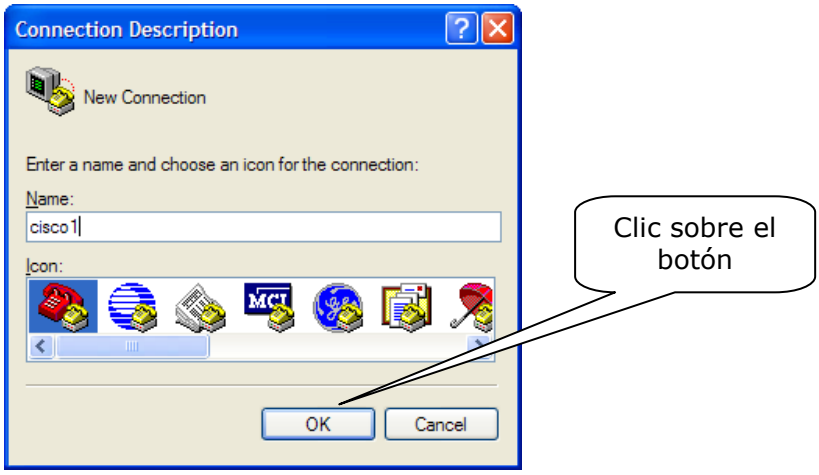
3.3 CONFIGURACIÓN DE EQUIPOS CISCO

3.3.1 INGRESO A LA CONFIGURACIÓN EN EQUIPOS CISCO

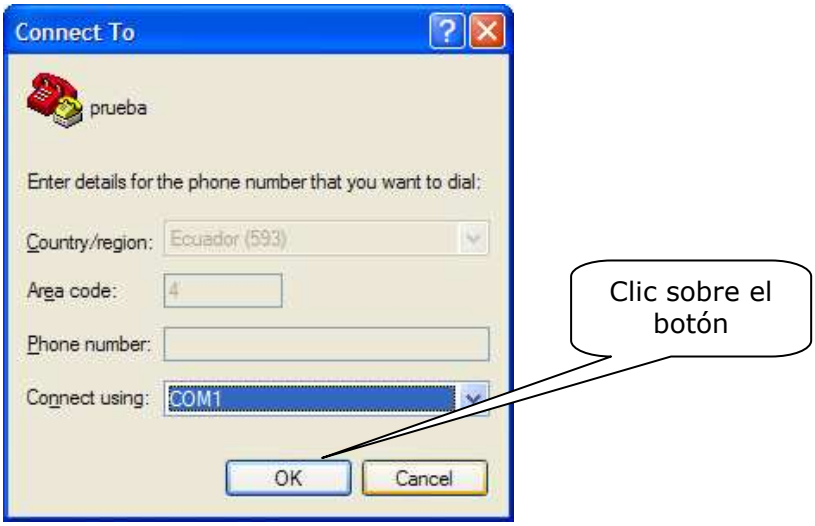
Para ingresar a la configuración de cualquier equipo Cisco, se debe acceder desde el Hiper Terminal:

Inicio
Programas
Accesorios
Comunicaciones
Hyper Terminal

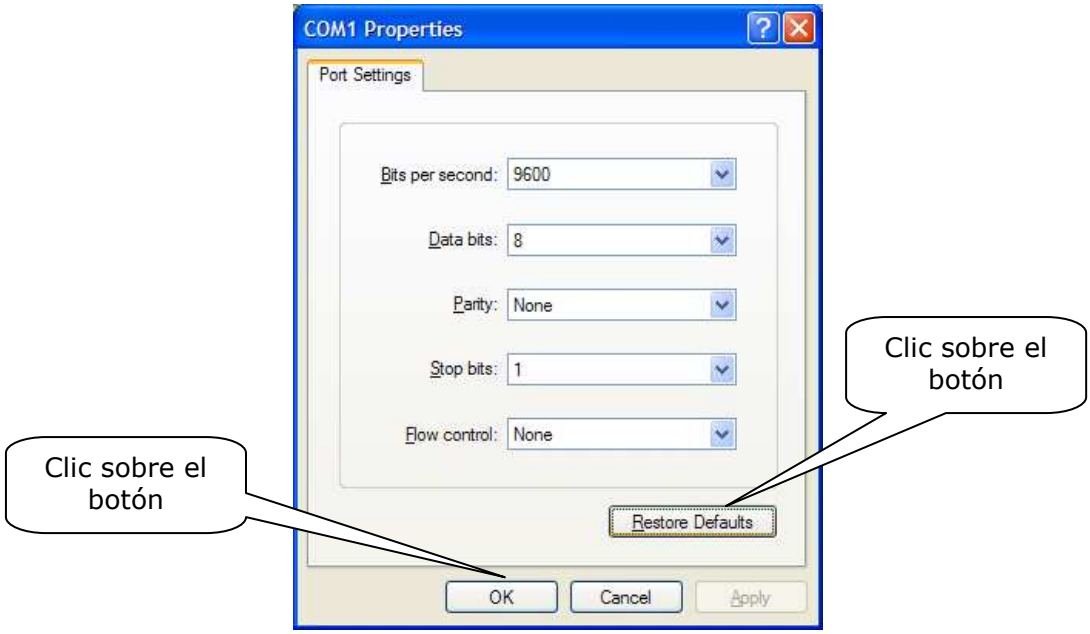
Asignar un nombre a la configuración.



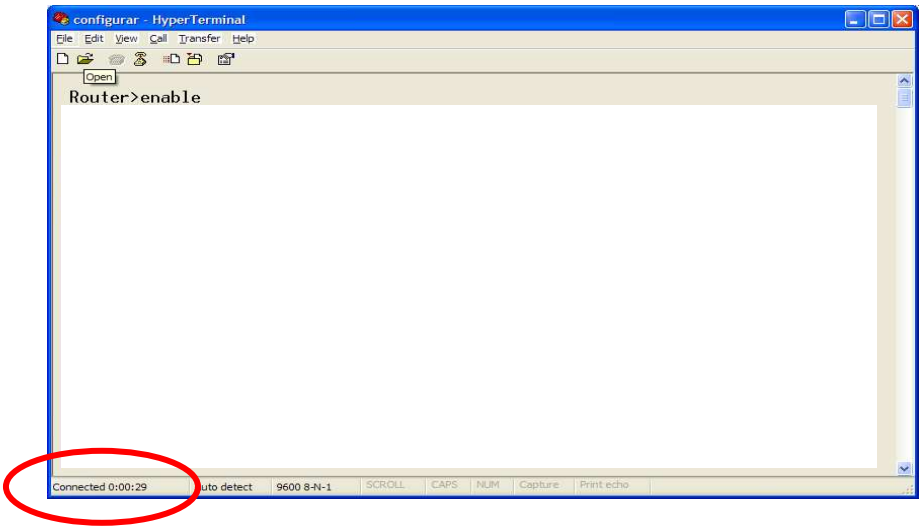
Seleccionar el puerto con el cual se realizara la conexión:



Restaurar valores por defecto:



Una vez realizados estos pasos se inicia la conexión a cualquier dispositivo Cisco.



Una vez iniciada la conexión se procede a seguir los comandos para la configuración.

3.3.2 USO DEL COMMAND-LINE INTERFACE

Los switches Catalist 2950 son soportados por el sistema operativo de Cisco IOS (Internetworking Operation system), aquí se describirá como usar el Command-Line Interface (CLI) para configurar este Software.

Los CLI se estructuran en los siguientes modos:

- User EXEC
- Privileged EXEC
- Global configuration
- Interface configuration
- Config-vlan
- VLAN configuration
- Line configuration

MODO USER EXEC

Luego de acceder al dispositivo, automáticamente entra al modo usuario, en este modo se ejecutan pocos comandos como para cambiar temporalmente la configuración, ejecutar pruebas básicas y listar información del sistema.

El prompt de este modo es el nombre del dispositivo seguido de “>” (switch>) y para salir usamos **logout**.

MODO PROVILEGED EXEC

Este modo tiene una protección con clave ya que aquí existen comandos que pueden cambiar la configuración del dispositivo, para ingresar a este modo digitamos el comando **enable**.

El prompt de este modo es el nombre del dispositivo seguido de “#” (switch#) y para salir usamos **disable**.

MODO GLOBAL CONFIGURATION

En este modo existen comandos que afectan las características del dispositivo completo, se usa el comando **configure** para ingresar al modo global, al ingresar este comando muestra un mensaje indicando la fuente del comando de configuración que puede ser Terminal, Memoria o Red.

Switch# **configure**
Configuring from terminal, memory, or network [terminal]?

- **configure terminal** Ingresa al modo de configuración global.
- **configure network** Copia a la RAM un archivo de configuración guardado en un servidor TFTP.
- **configure memory** Copia a la RAM un archivo de configuración guardado en la NVRAM.

Se puede especificar terminal o NVRAM como la fuente del comando como por ejemplo:

Switch# **configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.

Para salir del modo global y retornar al modo privilegio digitamos el comando **end** o **exit**, o presionamos **Ctrl.-Z**.

MODO INTERFACE CONFIGURATION

En este modo se modifican las operaciones de las interfaces, para ingresar a este modo usamos el comando **interface** *type_number.subif* y el nuevo prompt en este modo es Switch(config-if)#.

Para salir de este modo y regresar al modo global digitamos el comando **exit**, y para regresar al modo privilegio digitamos el comando **end** o presionamos Ctrl-Z.

MODO CONFIG-VLAN

Se usa este modo para configurar VLANs en rango normal (VLAN IDs 1 a 1005) , o cuando el modo VTP (VLAN Trunking Protocol) es transparent para configurar VLANs en rango extendido (VLAN IDs 1006 a 4094). Cuando el modo VTP es transparent la configuración VLAN y VTP es grabada en el archivo running configuration, y se puede guardar en el archivo de configuración de inicio del switch usando el comando en modo privilegio **copy running-config startup-config.**

La configuración de las VLANs IDs 1 a 1005 son guardadas en la VLAN database si VTP está en modo transparent o server. La configuración de VLANs extendidas no son grabadas en este VLAN database.

Ingrese el comando **vlan** *vlan-id* global para ingresar al modo config-vlan.

```
Switch(config)# vlan 2000
Switch(config-vlan)#
```

Para salir de este modo y regresar al modo global digitamos el comando **exit**, y para regresar al modo privilegio digitamos el comando **end,** todos los comandos excepto **shutdown** toman efecto cuando se salen de este modo.

MODO VLAN CONFIGURATION

Se pueden usar los comandos de VLAN configuration para crear o modificar parámetros de las VLANs 1 a 1005, se usa el comando en modo privilegio **vlan database** para acceder a este modo.

```
Switch# vlan database
Switch(vlan)#
```

MODO LINE CONFIGURATION

Los comandos en este modo permiten modificar la operación de una línea Terminal, se usan estos comandos para cambiar parámetros de terminales configurando línea por línea o por un rango de líneas.

Use el comando **line vty** *line_number* [*ending_line_number*] para ingresar en este modo.

```
Switch(config)# line vty 0 7
Switch(config-line)# ?
```

Para salir de este modo y regresar al modo global digitamos el comando **exit**, y para regresar al modo privilegio digitamos el comando **end** o presionamos Ctrl-Z.

3.3.3 CONFIGURACIÓN DE PASSWORD

Se configura el password de acceso a modo usuario para conexiones realizadas a través de telnet.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/z.
Switch(config)#line vty 0 15
Switch (config-line)#login
Switch(config-line)#password cisco
```

Con el mismo procedimiento puede configurarse un password para acceder por el puerto auxiliar. El puerto consola no requiere autenticación de password por defecto.

```
Switch(config-line)#exit
Switch(config)#line con 0
Switch(config-line)#login
Switch(config-line)#password cisco
```

Configurar un password de acceso al modo privilegiado encriptado.

```
Switch(config)#enable password [password]
```

Configura un password de acceso al modo privilegiado sin encriptar.

```
Switch(config)#enable secret [password]
```

3.3.4 CONFIGURACIÓN DEL NOMBRE DEL DISPOSITIVO

```
Switch(config)#hostname Swtich_2950
```

Este comando no admite la inclusión de espacios dentro del nombre del dispositivo.

```
Switch_2950(config)#banner motd #
Enter text message. End with the carácter #
Este es el switch 2950 de la LAN #
```

Este comando permite configurar un mensaje de bienvenida como en el caso de los routers.

3.3.5 CONFIGURACIÓN DE UNA DIRECCIÓN IP

En los switchs que corren lOS la dirección IP identifica a una VLAN. Por defecto, todos los puertos del switch están asignados a la VLAN 1 y esta es la VLAN de manejo, por lo que operativamente al configurar la IP de la VLAN 1 se asigna una IP para manejo del switch.

En los swtiches Catalyst 2950, la VLAN es tratada como una interfase virtual, por lo que se accede a ella con el comando **interface**. (No se está configurando una IP en una interfase, eso es imposible en un switch capa 2).

```
Swtich 2950(config)#interface v1an1
Switch 2950(config-if)#ip address 172.16.5.2 255.255.255.0
```

Asigna una dirección IP y máscara de subred a la VLAN.

```
Switch 2950(config-if)#no shutdown
Switch-2950(config-if)#exit
Switch-2950(config)#ip defau1t-gateway 172.16.5.1
```

Nota: El default-gateway se configura en el modo de configuración global.

3.3.6 CONFIGURACIÓN DE INTERFASES

A continuación se indica como configurar las distintas interfaces que tiene el Switch.

```
Switch_2950(config)#interface fastEthernet 0/1
```

Permiten acceder al sub-modo configuración de interfases Fast Ethernet.

```
Switch_2950(config-if)#description puerto servidor 2
```

Permite ingresar una descripción del puerto que tendrá significación local.

3.3.7 VERIFICACIÓN DE LA CONFIGURACIÓN

Los siguientes son algunos comandos que permiten revisar las configuraciones del switch.

```
Switch_2950#show interfaces
Switch_2950#show running-config
Switch_2950#show version
```

3.3.8 BORRAR LA CONFIGURACIÓN

Para borrar la configuración almacenada en la NVRAM se usa el siguiente comando:

```
Switch_2950#erase startup-config
Erasing the nvram filesystem Hili remove all files! Continue? [confirm] [OK]
Erase the nvram:complete
```

Borra la copia del archivo de configuración de respaldo almacenada en la NVRAM.

Los switches Catalyst 2950 al igual que los routers tienen tanto configuración activa (RAM) como configuración de respaldo (NVRAM).

3.3.9 CONFIGURACION DE VTP

Es un protocolo usado para configurar y administrar VLAN´s en equipos Cisco. VTP opera en 3 modos distintos: - Cliente - Servidor – Transparente.

Modos VTP

Servidor Comparte la información con los demás dispositivos VTP que integran el mismo dominio VTP. Es el modo en el que se crean VLAN´s y se realizan cambios. Toda modificación en el switch servidor es transmitida a todo el dominio. Es el estado por defecto de todo switch Cat 1900.

Cliente Envía y recibe información VTP, pero no puede introducir ningún cambio.

Transparente Envía y recibe información de VTP, pero no la incluye en su base de datos. No participa del dominio VTP.

Se debe comenzar configurando VTP a fin de evitar posteriores inconvenientes con la base de datos de VLAN, ya que todos los switches Catalyst 2950 son servidores VTP por defecto.

Primero verificamos la configuración del protocolo VTP en el switch. El modo servidor es el modo por defecto.

```
Switch_2950#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLAN supported locally : 254
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Diaabled
VTP Traps Generation            : Diaabled
MD5 digest                      : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5
Configuration last modified by 0.0.0.0 at 0-0-00  00:00:00
Switch_2950#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
```

Para activa el dispositivo en modo cliente, servidor o transparente ejecutamos el siguiente comando:

```
Switch_2950(config)#vtp mode [client / server / transparent]
```

Para asigna el switch a un dominio VTP nombrado ejecutamos el siguiente comando:

```
Switch_2950(config)#vtp domain [name]
```

3.4 IMPLEMENTACIÓN DE VLAN´S

A continuación se presenta como configurar una VLANs en general y luego como se configuran las VLANs del MAG.

3.4.1 CONFIGURACIÓN DE VLANs

En los switches Catalyst 2950 hay un modo particular para configurar las VLANs, es el modo VLAN, al que se debe ingresar para cualquier actividad de configuración relacionada con las VLANs.

Los pasos para crear una VLAN son los siguientes:

- Primero el Switch debe estar en modo VTP “Server”, o “Transparent”.

- Crea una VLAN y definir su nombre.
- Asignar puertos a la VLAN.
- Configurar un puerto troncal para enlazar las VLAN´s.
- Configuramos el tipo de encapsulamiento.
- Grabamos la configuración.

Para crea una VLAN y definir su nombre utilizamos el siguiente comando:

Switch 2950#**vlan database**
Switch_2950(vlan)#**vlan [#] name [nombre]**
VLAN # added :
Name: nombre

Aplicamos los cambios y salimos del modo VLAN para que los cambios realizados tengan efecto.

Switch_2950(vlan)#**apply**
Switch_2950(vlan)#**exit**
APPLY completed.
Exiting....

Para remover una VLAN de la base de datos ejecutamos:.

Switch_2950#**vlan database**
Switch_2950(vlan)#**no vlan [#]**
Deleting VLAN #.. .

Para revisar las VLANs creadas en un switch ejecutamos:.

Switch_2950#**show vlan**

VLAN	Name	Status	Ports
1	default	active	FaO/1, FaO/2, FaO/3, FaO/4, FaO/5
2	Prueba	active	FaO/6, FaO/7, FaO/8, FaO/9, FaO/10, FaO/11
1002	fddi-default	active	
1003	token~ring-default	active	
1004	fddinet-defau1t	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	PaIent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500						0	0
2	enet	100002	1500						0	0
1002	fddi	101002	1500						0	0
1003	tr	101003	1500						0	0
1004	fdnet	101004	1500				ieee	-	0	0
1005	trnet	101005	1500				ibm		0	0

```
Switch_2950#show vlan brief
VLAN Name              Status    Ports
1    defau1t           active    FaO/1, FaO/2, FaO/3, FaO/4, FaO/5
2    Prueba            active    FaO/6, FaO/7, FaO/8, FaO/9, FaO/10,
FaO/11
1002 fddi-defau1t      active
1003 token-ring-defau1t active
1004 fddinet-default   active
1005 trnet-defau1t     active
```

Para asignar un puerto a una VLAN de modo estático ejecutamos:

```
Switch_2950#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Switch_2950(config)#interface fastEthernet 0/4
Switch_2950(config-if)#switchport access vlan [#]
```

Para Remover a este puerto de la VLAN # ejecutamos:

```
Switch_2950(config-if)#no switchport access vlan [#]
```

La interfase removida no es asignada automáticamente a ninguna VLAN, y estará deshabilitada. Para que vuelva a ser utilizable se la deberá incorporar a la VLAN 1 u otra.

3.4.2 CONFIGURACION DE PUERTOS TRONCALES

Para cambiar el modo del puerto de acceso a troncal, y permitir su operación como puerto troncal ejecutamos el siguiente comando:

```
Switch_2950(config)#interface fastEthernet 0/1
Switch_2950(config-if)#switchport mode [access/multi/trunk]
Switch_2950(config-if)#switchport mode trunk
```

Para configura el puerto troncal para utilizar encapsulación ISL u 802.1q ejecutamos:.

```
Switch_2950(config-if)#switchport trunk encapsulation [isl/dot1q]
```

Nota: No todos los switches Catalyst tienen la posibilidad de optar por una u otra encapsulación.

Para cambia el modo del puerto de acceso a multi-VLAN, para permitir el tráfico de varias VLAN´s por este puerto ejecutamos el siguiente comando.

Switch_2950(config-if)#**switchport mode multi**

Se trata de un puerto que participa de múltiples VLAN´s, no de un puerto troncal.

Para asigna un puerto múltiple a las VLAN´s que se enumeran se ejecuta:

Switch_2950(conrig-if)#**switchport multi vlan [#] , [#] , [#]**

Para verificar el estado de un puerto troncal ejecutamos:

Switch_2950#**show interface fastEthernet 0/1 switchport**
Narne: FaO/1
Operational Mode: trunk
Adrninistrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: isl
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: NONE
Priority for untagged frarnes: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none

Esto nos indica que el puerto está en modo troncal y además todas sus características.

Para mostrar todas las interfaces Trunk digitamos:

Switch_2950#**show interface trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1
Fa0/2	on	802.1q	trunking	1

Todos estos comandos han afectado la configuración de la RAM, si apagamos el ruteador se perderán. Si queremos que estos cambios se graben permanentemente en la NVRAM ejecutamos el siguiente comando:

Switch_2950#**wr mem**
Building configuration...
[OK]
Switch_2950#

3.4.3 CONFIGURACIONES DE LOS SWITCHS DEL MAG

Para las VLAN´s del MAG se considerará la implementación por puerto ya que son las más comunes.

La tabla 3.11 resume las VLAN´s que se instalarán y configurarán según el capítulo 2.

NOMBRE	IP	SubRed	MÁSCARA	MAX. # Host
VLAN1	172.16.0.0	172.16.29.0	255.255.255.0	254
VLAN2	172.16.0.0	172.16.28.0	255.255.255.0	254
VLAN3	192.168.254.0	X	255.255.255.0	254
VLAN4	192.168.252.0	X	255.255.255.0	254
VLAN5	192.168.5.0	X	255.255.255.0	254
VLAN6	192.168.1.0	X	255.255.255.0	254

Tabla 3.11 Valores de VLAN´s a configurar.

A continuación se detallan los comandos requeridos para configurar un switch Cisco Catalist 2950 de la capa de acceso en el piso 6.

Switch>
Switch>**enable**
Switch#
Switch#**configure terminal**
Enter configuration commands, one per line. End with *CNTL/z.*
Switch(config)#
Switch(config)#**enable password CISCO**
Switch(config)#
Switch(config)#**hostname Mag_sw2950_p6.2**
Mag_sw2950_p6.2(config)#
Mag_sw2950_p6.2(config)#**banner motd #**
Enter text message. End with the carácter #
Switch de Acceso del piso 6 #
Mag_sw2950_p6.2 (config)#**exit**
Mag_sw2950_p6.2#
Mag_sw2950_p6.2#**show vtp status**
VTP Version : 2
Configuration Revision : 0

Maximum VLAN supported locally : 254
Number of existing VLANs : 5
VTP Operating Mode : Transparent
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Diaabled
VTP Traps Generation : Diaabled
MD5 digest : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Mag_sw2950_p6.2#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z
Mag_sw2950_p6.2(config)#**vtp mode server**
Mag_sw2950_p6.2 (config)#**exit**
Mag_sw2950_p6.2#
Mag_sw2950_p6.2#**vlan database**
Mag_sw2950_p6.2(vlan)#**vlan 1 name vlan 1**
VLAN 1 added :
Name: vlan 1
Mag_sw2950_p6.2(vlan)#**vlan 2 name vlan 2**
VLAN 2 added :
Name: vlan 2
Mag_sw2950_p6.2(vlan)#**vlan 3 name vlan 3**
VLAN 3 added :
Name: vlan 3
Mag_sw2950_p6.2(vlan)#**apply**
Mag_sw2950_p6.2(vlan)#**exit**
APPLY completed.
Exiting....
Mag_sw2950_p6.2#
Mag_sw2950_p6.2#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/1**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 2**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/3**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 3**
Mag_sw2950_p6.2(config-if)#**description Juana Tejada**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/4**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 3**
Mag_sw2950_p6.2(config-if)#**description Remigio Jara**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/5**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 3**
Mag_sw2950_p6.2(config-if)#**description Impresora SIA**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/6**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 3**
Mag_sw2950_p6.2(config-if)#**exit**

Mag_sw2950_p6.2(config)#**interface fastEthernet 0/7**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 2**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/8**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 3**
Mag_sw2950_p6.2(config-if)#**description Martha Varela**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/9**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 2**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/12**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 2**
Mag_sw2950_p6.2(config-if)#**description Ma. Eugenia Garcia**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/14**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 2**
Mag_sw2950_p6.2(config-if)#**description Gustavo Sevillano**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/15**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 3**
Mag_sw2950_p6.2(config-if)#**description Rolando Gonzalez**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/16**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 2**
Mag_sw2950_p6.2(config-if)#**description Impresora Ing. Velasquez**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/17**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 2**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/18**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 3**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/19**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 2**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/20**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 3**
Mag_sw2950_p6.2(config-if)#**description telefono PRECIOS**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/21**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 2**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/22**
Mag_sw2950_p6.2(config-if)#**switchport access vlan 2**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**interface fastEthernet 0/24**
Mag_sw2950_p6.2(config-if)#**switchport mode trunk**
Mag_sw2950_p6.2(config-if)#**switchport trunk encapsulation dot1q**
Mag_sw2950_p6.2(config-if)#**exit**

Mag_sw2950_p6.2(config)#
Mag_sw2950_p6.2(config)#**interface v1an1**
Mag_sw2950_p6.2(config-if)#**ip address 192.168.254.62 255.255.255.0**
Mag_sw2950_p6.2(config-if)#
Mag_sw2950_p6.2(config-if)#**no shutdown**
Mag_sw2950_p6.2(config-if)#**exit**
Mag_sw2950_p6.2(config)#**ip defau1t-gateway 192.168.254.1**
Mag_sw2950_p6.2 (config)#**exit**
Mag_sw2950_p6.2#
Mag_sw2950_p6.2#**wr mem**
Building configuration...
[OK]
Mag_sw2950_p6.2#

Las configuraciones de los Switches del MAG se muestran en el anexo 4.

3.4.4 CONFIGURACIÓN DE LOS ROUTERS CISCO.

En este punto se explicarán conceptos básicos de la configuración de routers con sistema operativo IOS del fabricante de routers Cisco System y se detallarán las configuraciones utilizadas en este proyecto.

Al igual que en los switches, desde los modos USER EXEC y PRIVILEGED EXEC no podemos modificar la configuración del router, para hacerlo debemos pasar del modo PRIVILEGED EXEC al modo de configuración general (CONFIGURE). Desde allí podemos configurar aspectos generales del funcionamiento del router o pasar a modos de configuración específicos de cada interfaz, algoritmo de encaminamiento, etc.

Empezaremos configurando una clave para el ruteador.

Router> **enable**
Router# **config terminal**
Router(config)# **enable secret PASSW**
Router(config)# **exit**
Router# **disable**
Router> **enable**
pass: ********** (PASSW)
Router#

Como ya hemos mencionado, los cambios de configuración que se realicen en el modo de configuración global o específico se guardan sobre un archivo de configuración residente en la RAM del router llamado “running-config”. Este fichero puede ser visualizado desde el modo de configuración privilegiado con el comando “**show running-config**”. Si el router se apagase, estos cambios se perderían al estar almacenados en RAM. Para que no se pierdan y pasen a estar permanentemente guardados en una memoria NVRAM hay que copiar el archivo “running-config” (RAM) en el archivo “startup-config” (NVRAM). Ello se puede hacer desde el modo PRIVILEGED EXEC con el comando “**copy running-config startup-config**”.

Podemos consultar el estado de un router mediante los comandos “**show**”. Dependiendo del tipo de información que queremos consultar, el comando es ejecutable desde modo USER EXEC o bien necesitamos los privilegios del modo PRIVILEGED EXEC. Por ejemplo:

“**show running-config**” muestra el fichero de configuración que está activo en el router

“**show startup-config**” muestra el fichero de configuración que está grabado en la NVRAM

“**show ip** <**parameter**>” muestra los parámetros asociado a la configuración del protocolo IP. Por ejemplo, la tabla de encaminamiento IP se consulta con “**show ip route**”

“**show interface eth0**” muestra los parámetros asociados al interface Ethernet eth0

Desde el modo de configuración podemos pasar a configurar las interfaces. Por ejemplo, para configurar una interface ethernet podemos hacer:

```
Router# configure terminal
Router(config)# interface eth0
Router(config-if)# ip address @IP MASK
Router(config-if)# no shutdown
Router(config-if)# exit
Router#
```

El comando "**no shutdown**" es necesario para activar la interfaz. Por defecto, al arrancar el router todas los interfaces están desactivadas. El comando "**shutdown**" en su defecto desactivaría administrativamente una interfaz.

A continuación vemos un ejemplo de configuración del encaminamiento estático usando el comando "**ip route**".

Router(config)# **ip route @IPnet MASK @IPgw**

La primera dirección es la dirección de red destino. A continuación escribimos la máscara asociada a esa red. La tercera dirección corresponde a la interfaz del router por donde se establece la ruta (gateway por defecto).

Las configuraciones del Router y del Firewall del MAG se muestran en el anexo 4.

3.5 ANÁLISIS DE COSTOS

A continuación se realizará el análisis de costos referente a instalaciones de ser necesarias, en caso de requerirse adicionar estaciones de trabajo. Por esta razón se ha considerado los costos de red de datos, equipos activos de red, costos por servicios profesionales por concepto de configuración, diseño y capacitación. El objetivo de este análisis, es determinar la cantidad de recursos económicos necesarios para el futuro crecimiento de la red de datos.

Los costos por cada nuevo punto de red de datos categoría 5e Alcatel se detalla en la tabla 3.12.

No. Parte	CANT.	DESCRIPCION	P. UNIT US $
ACS-100.464	1	FTP CAT5E350 0,5MM PVC 1000M REEL	$0,44
ACS-200.105	**1**	TO 45x45 pearl white surface mounted	$3,90
ACS-461.101	**1**	Omega 45 outlet 1RJ45 unscreened ivory shutters	$7,67
ACS-500.101	**1**	OMEGA 1HU PP 24 RJ45 UNSCREEN. + CLIP-ON(Proporcional por punto)	$4,58
QST NPP-1103	**1**	Patch cord de 3 pies cat. 5e (QUEST)	$1,53
QST NPP-1107	**1**	Patch cord de 7 pies cat. 5e (QUEST)	$2,05
	1	**DIRECCION TECNICA DEL PROYECTO, INSTALACION, PRUEBAS Y CERTIFICACION** incluye : CANALETAS, TUBERIA EMT , ACCESORIOS, UNIONES Y MATERIALES DE SUJECION	$31,00
		COSTO TOTAL POR PUNTO	**$51,17**

Tabla 3.12 Costo por punto de Cableado Estructurado Cat 5e.

Si consideramos que son 125 puntos adicionales, entonces podemos encontrar que el costo total por cableado estructurado categoría 5e es USD$ 6.396,25.

Para el análisis de costos de los elementos activos de la red, se consideraron las características de los equipos que se detalla en el punto 3.1 de este capitulo, además se recomienda tener un stock de equipos, mismos que servirán para contingencia y pruebas.

A continuación en la tabla 3.13 se detallan los costos de estos equipos activos.

ITEM	DESCRIPCION	CANT.	VALOR UNITARIO (USD)	VALOR TOTAL (USD)
1	Switch Catalyst 2950-24	7	1.200,00	8.400,00
2	Switch Catalyst 2950-48	2	2.100,00	4.200,00
3	Switch Catalyst 3548-XL-EN	7	2.400,00	16.800,00
4	Cisco WS-G5484 - Cisco SX GBIC Module	7	175,00	1.225,00
5	Cisco WS-6006	1	9.200,00	9.200,00
VALOR TOTAL EN EQUIPOS ACTIVOS				39.825,00

Tabla 3.13 Costos de Elementos Activos.

Los costos referenciales del soporte técnico de un profesional certificado en redes de acuerdo al mercado nacional vigente es el que se detalla a continuación en la tabla 3.14.

ITEM	DESCRIPCION	CANTIDAD (HORA/TECNICA)	VALOR UNITARIO (USD)	VALOR TOTAL (USD)
1	Diseño y Configuración de VLAN´s en los equipos activos existentes al momento.	30	40.00	1200.00
2	Pruebas de conectividad a nivel de capa 2 y capa 3.	15	40.00	600.00
3	Capacitación del personal del área de comunicaciones para configurar, mantener y administrar la red del MAG.	20	40.00	800.00
4	Apoyo para la elaboración de la documentación que sirva de instructivo para los procedimientos de modificación, administración y control de la red LAN.	20	40.00	800.00
VALOR TOTAL POR SERVICIOS PROFESIONALES				3.400,00

Tabla 3.14 Costos por servicios profesionales

En la tabla 3.15 se resume el costo total de la implementación del presente proyecto.

ITEM	DESCRIPCION	VALOR TOTAL (USD
1	Cableado estructurado	6.396,25
2	Elemento activo	39.825,00
3	Servicios profesionales	3.400,00
	VALOR TOTAL	49.621,25

Tabla 3.15 Costo total del proyecto

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

3.1 CONCLUSIONES

- Este tipo de configuraciones en tres capas no es muy común en nuestro país debido a su alto costo y a que esta configuración se recomienda en instalaciones de mas de 500 usuarios.

- Hay topologías muy diversas para las redes LAN (bus, estrella, anillo) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte casi transparente para los equipos que la utilizan.

- Además de proporcionar un acceso compartido, la LAN del MAG también proporcionan al usuario multitud de funciones avanzadas. Hay paquetes de software de gestión para administrar la configuración de los equipos en la LAN, la administración de los usuarios y el control de los recursos de la red.

- El Firewall divide a la red del MAG en tres zonas claramente definidas, la Outside que es la que está hacia la WAN, la Inside que es la que está hacia la LAN y es la que hay que proteger, y la DMZ o zona desmilitarizada que es una zona con una protección media y donde se encuentran los servidores que tienen acceso a la WAN.

- Los servidores que se encuentran en la zona desmilitarizada pertenecen a la VLAN 4 principalmente por seguridad, para que ningún usuario no autorizado pueda ingresar a ellos y también para que los ataques desde afuera sean mas aislados hacia el sector de la LAN.

- El protocolo que permite crear una VLAN con equipos conectados a diferentes switches es el spanning-tree.

- Un switch utiliza el protocolo de spanning-tree en todas las VLAN basadas en Ethernet y Fast Ethernet. El protocolo de spanning-tree detecta y elimina loops colocando algunas conexiones en modo de espera, que se activa en el caso de una falla de conexión activa.

- La aplicación de VLAN´s, permite crear grupos de trabajo como si estos grupos pertenecieran a diferentes switches a pesar de que estén conectados al mismo switch, permitiendo la utilización adecuada de todos los puertos, mejorando la seguridad y administración entre los diferentes grupos de trabajo creados (VLAN´s).

- Una de la características tomadas en cuenta para clasificar si los Switches son de Acceso, Distribución o Núcleo, es el método de envío de paquetes que ellos soportan como son Store&Fordward y Cut-Through. Para Switch de acceso se escoge con método Store&Fordward ya que con esta tecnología se realiza chequeo de errores y los frames erróneos son descartados. Si el CRC es erróneo el frame es descartado, si el frame es Runt (menor que 64 bytes incluyendo el CRC) o Giant (mayor que 1518 incluyendo el CRC), también es descartado, si no hay error el frame es enviado a su destino. En cambio para Switches de Distribución o Núcleo se escoge con tecnología Cut-Through por no necesitar ya chequeos de error, en este modo de operación el Switch copia solamente la dirección de destino (los primeros 6 bytes seguidos del preámbulo), luego verifica la dirección en la tabla de direcciones (MAC address) y determina la puerta o interfaz de salida, finalmente el frame es enviado a su destino. Estos métodos son propios de la construcción de cada switch y no se los puede configurar.

- Al usar la tecnología Store&Fordward se tiene la ventaja de que verifica el CRC del frame antes de enviarlo al destino, filtra los frames Runts o Giants y con CRC erróneo, soporta puertas LAN con distintas velocidades de operación, pero en cambio tiene mayor latencia (Latencia = largo del frame + tiempo de procesamiento), más características u opciones de verificación incrementan la latencia.

- Al usar la tecnología Cut-Through se tiene la ventaja de tener baja latencia, es apropiado en entornos de operación de una sola velocidad, pero en cambio no detecta ni descarta frames dañados. La latencia se incrementa cuando existe congestión o las velocidades de operación son distintas.

- Como podemos observar, la disponibilidad de la red no se puede asegurar al 100% ya que no existe redundancia en la capa Acceso ni en la capa de Distribución, pero en la capa Core contamos con un equipo con un 95% de redundancia lo que nos asegura una buena disponibilidad en esa capa y que por cierto es la más importante en toda la red.

- Para controlar el tráfico entre las VLAN se utiliza las listas de control de acceso (ACL, Access Control List) las cuales nos permiten establecer los accesos entre las diferentes VLAN´s, estas listas se las crean o se configuran en el Router.

3.2 RECOMENDACIONES

- Los equipos activos de la red del MAG, cumplen con todos los estándares de la industria, permitiendo la administración y configuración de sus equipos para cumplir con los requerimientos de comunicación, estando dependiente del grado de conocimiento y experiencia del personal que administra la red.

- Por las características de reemplazos constantes en la cúpula administrativa del MAG, es indispensable la elaboración de documentación que sirva como instructivo de procedimientos para modificaciones, administración y control de la red. Así como también se debe registrar un histórico de las soluciones dadas y de la evolución de la red.

- Cuando se diseñe y se implemente una red de datos se lo debe hacer en lo posible con equipos activos, (switch, router, etc.), de una misma marca o fabricante con la finalidad de poder explotar al máximo todos los beneficios que nos da cada uno de ellos, porque cuando se utiliza equipos de diferentes fabricantes algunas características técnicas no son compatibles con las de otro, pese a que los dos equipos estén estandarizados para realizar una función específica, por ejemplo creación de VLAN´s con el Estándar 802.1Q.

- Para el direccionamiento IP de una Intranet se debe utilizar o hacer referencia al estándar de direcciones privadas de la RFC 1597, que nos explica la correcta utilización de las direcciones IP, y nos sugiere hacer uso de las recomendaciones de la IANA (autoridad de asignación de números de Internet).

- Los puertos no utilizados de los switches de Acceso y Distribución deben estar asignados a una VLAN que no tenga uso como por ejemplo una llamada "guest", en la misma que se ha de negar todos los servicios de la red.

- En el desarrollo de la investigación, implantación y configuración de las VLANs, es necesario planificar y seguir un procedimiento organizado y bien estructurado de tal forma que garantice el éxito del proyecto, cumpliendo tiempos de ejecución, predicción de imprevistos, distribución de los recursos, capacitación del personal.

- Se recomienda para instituciones estatales seguir un lineamiento tecnológico a largo plazo para que tenga un impacto trascendente en el desarrollo institucional y no sea cuestión de los gobiernos de turno cambiar estos lineamientos olvidándose de lo hecho anteriormente.

- Luego de la terminación de este proyecto, se recomienda que cualquier crecimiento de cualquier institución adscrita al ministerio o del mismo ministerio sea canalizada o regulada por el personal de administración de la red del Ministerio para que exista el crecimiento estructurado esperado y para lo cual se creo esta red.

- Para mantener la disponibilidad de la red se recomienda colocar Switches redundantes en la capa de Distribución con links redundantes y mantener Switches de respaldo para la capa de Acceso.

BIBLIOGRAFÍA

TANENBAUM, Comer. **Teorías de Comunicación de Datos y Redes de Datos**, 2nd ed. Prentice Hall, 1989.

Sánchez Paucar Edwin Patricio, **METODOLOGIA PARA EL DISEÑO DE REDES VIRTUALES VLAN´S**, 2000

Ing. José Joskowicz, **REDES DE DATOS** Instituto de Ingeniería Eléctrica, Facultad de Ingeniería Montevideo, Uruguay Agosto 2004 Versión 2

Eduardo Collado Cabeza, **Las VLAN**, 11 de Enero de 2004 [pdf]

María Dolores Cerini – Pablo Ignacio Prá, **PLAN DE SEGURIDAD INFORMÁTICA,** Octubre 2002

Estandarización de Redes LAN
http://www.die.udec.cl/~redes/apuntes/myapuntes/node75.html#TB:WG802 Marzo del 2006

Guía de arquitectura de referencia de Internet Data Center
http://www.microsoft.com/spain/technet/guias/internet_datacenter.mspx Agosto del 2006

Seguridad en una Red http://www.monografias.com/trabajos6/sein/sein.shtml Septiembre del 2006

XPEDITION, **User Reference Manual**, Marzo del 2004 [pdf]

IEEE 802.1q – VLAN http://standards.ieee.org/getieee802/802.1.html

IEEE 802.1p: LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization
http://www.javvin.com/protocol8021P.html Abril del 2006

Spanning Tree Protocol in IEEE 802.1D http://www.javvin.com/protocolSTP.html Marzo del 2006

GLOSARIO DE TÉRMINOS

B

Backbone: La columna vertebral de la Red.

Backup: Aplicación de copia de seguridad de ficheros, carpetas o unidades completas que permite dividir la información o ficheros en varios disquetes y que además la comprime.

Bit: (binary digit): Unidad básica de información representada por ceros y unos que se van sucediendo para conformar los distintos significados.

Browser: Navegador para poder visualizar las páginas Web en Internet.

Byte: Medida básica de capacidad en informática. Comprende 8 bits o interruptores, cada uno de los cuales puede conmutar en dos posiciones ON y OFF.

C

Caché: Carpeta o memoria intermedia que almacena temporalmente los archivos del equipo.

Correo electrónico: Mensajes, documentos, archivos que se envían personas a través de Internet o de una red.

Cortafuegos (firewall): Programa que protege a una red de otra red.

D

Dirección IP: Cadena numérica que identifica a una máquina en una red IP.

DNS: Sistema de Nombres por Dominio utilizado en Internet y basado en una estructura jerárquica y mediante el cual comunicamos con otro ordenador que puede encontrarse en otra parte del mundo.

Dominio: Grupo de equipos conectados en red que comparten información y recursos.

E

Extranet: Red basada en Internet de una compañía en la que comparte información y comunicación con agentes externos.

F

Firewall: Dispositivos de seguridad a entradas no autorizadas.

FTP (Protocolo de Transferencia de Ficheros): Transferir ficheros entre ordenadores en Internet.

G

Gateway (Puerta de acceso): Dispositivo que permite conectar entre sí dos redes normalmente de distinto protocolo o bien un servidor a una red.

Gigabyte (GB): Medida de 1.000 Mb (unos 1.000 millones de caracteres).

Grupos de trabajo: Conjunto de equipos conectados en red y que comparten los mismos recursos.

H

Host: Anfitrión, es cualquier ordenador que tiene un número IP y que puede tanto enviar como recibir información por una red.

HTTP: Protocolo de Transferencia de Hipertexto o entorno gráfico de las páginas Web.

Internet: Red de redes mundial. Telaraña o entramado mundial. También llamada World Wide Web (WWW), conjunto de redes que permiten la comunicación de millones de usuarios de todo el mundo.

Intranet: Red privada dentro de una organización que utiliza los protocolos propios de Internet.

IP: Dirección numérica y única de cada ordenador en Internet.

M

Módem (modulador/demodulador): Dispositivo que transmite datos desde un equipo a otro a través de la línea telefónica.

P

Password: Clave secreta personal.

Proveedor de Servicios Internet (ISP): Organización que proporciona acceso a Internet mediante una tarifa y que nos ofrece una serie de servicios.

Proxy: Servidor que realiza la conexión a Internet y que sirve de puerta de entrada a los ordenadores cliente.

S

Servidor: Equipo que controla el acceso de los usuarios a una red y les da servicio e información.

T

TCP/IP: Protocolo de Internet (Protocolo de Control de Transmisión/Protocolo Internet) que específica cómo se transmiten los datos en Internet para que todos los sistemas hablen el mismo idioma en Internet.

Telnet: Servicio que permite la conexión remota con cualquier ordenador de la red situado en cualquier parte del mundo como si de una terminal más se tratase.

W

WAN (Wide Area Network): Red pública de área extensa, no tiene límites físicos.