PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

SEDE AMBATO

DEPARTAMENTO DE INVESTIGACION, POSTGRADOS Y AUTOEVALUACION

TEMA:

PROPUESTA DE REINGENIERIA DE LA RED INFORMÁTICA CON CALIDAD DE SERVICIOS PARA EL HONORABLE CONSEJO PROVINCIAL DE TUNGURAHUA

Plan de trabajo de tesis de grado previo a la obtención del título de Maestría en Gerencia Informática con mención en Redes y Desarrollo de Software.

AUTOR

MARCELO PATRICIO TOALOMBO MONTERO

DIRECTOR

Msc. Diego Avila.

Ambato – Ecuador

Julio, 2008

Pontificia Universidad Católica del Ecuador

Sede Ambato

HOJA DE APROBACION

DEPARTAMENTO DE INVESTIGACION, POSTGRADOS Y AUTOEVALUACION

TEMA:

PROPUESTA DE REINGENIERIA DE LA RED INFORMATICA CON CALIDAD DE SERVICIOS PARA EL HONORABLE CONSEJO PROVINCIAL DE TUNGURAHUA

AUTOR

MARCELO PATRICIO TOALOMBO MONTERO

Diego Avila, Ing. Msc
DIRECTOR DE TESIS
f:_____

Patricio Medina, Ing. Msc
CALIFICADOR
f:_____

Andrés López, Ing. Msc
CALIFICADOR
f:_____

Telmo Viteri, Ing. Msc
DIRECTOR DIPA
f:_____

Pablo Poveda Mora, Dr.
SECRETARIO GENERAL PUCESA
f:_____

DECLARACION DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, TOALOMBO MONTERO MARCELO PATRICIO portador de la cédula de ciudadanía No. 180286263-9 declaro que el contenido de este proyecto de investigación previo para la obtención del título de Magister en Gerencia Informática con mención en Redes y Desarrollo de Software, tanto en datos obtenidos como en resultados alcanzados son absolutamente originales, auténticos y personales.

Por lo tanto declaro que la investigación enmarcada en el diseño de la tesis es absolutamente original, auténtica y personal; en tal virtud, el contenido, efectos legales y académicos que se desprenden del trabajo de tesis son y será de mi exclusiva responsabilidad legal y académica.

Ing. Marcelo Toalombo
C.I. 1802862639

AGRADECIMIENTO

Agradezco a mi madre y hermanos por su apoyo e incentivo para mi desarrollo personal y profesional.

A mis amigos que han sido mi apoyo en mis estudios y en los difíciles momentos.

A mis compañeros de maestría que supieron brindarme sus conocimientos y experiencias, para poder realizar este proyecto, y a la Pontificia Universidad Católica del Ecuador Sede Ambato que me dio la oportunidad de especializarme e incrementar mis conocimientos en lo que concierne a la gestión de proyectos informáticos y redes.

También exteriorizo un agradecimiento especial a mí Director de Tesis ya que gracias a su profesionalismo y experiencia me ha sabido orientar y dirigir en el desarrollo de este proyecto de investigación.

Adicionalmente agradezco al H. Consejo Provincial de Tungurahua mi lugar de trabajo, que me ha servido de campo de aprendizaje y desarrollo profesional y que me ofrece la oportunidad para formarme cada día como persona en conjunto con mis amigos y compañeros de trabajo.

Ing. Marcelo Toalombo

DEDICATORIA

Dedico el presente trabajo de investigación a mí abnegada Madre, quien con su amor, sacrificio, y paciencia, ha sabido Orientarme para caminar por las difíciles etapas de mi vida, Nexo que ha sido vital en mis estudios; y a mis queridos Incondicionales hermanos quienes con su cariño siempre se han Ufanado en incentivar mi desarrollo como persona y así terminar Mi carrera profesional con éxito y satisfacción.

Y especialmente a mi pequeño "dmonium", mi sobrinito William Alejandro que me ha alegrado infinitamente con su compañía

Marcelo Toalombo

RESUMEN

Este Proyecto muestra un análisis de la situación actual de la plataforma tecnológica de red y de los servicios informáticos que posee el Honorable Consejo Provincial de Tungurahua, de cómo están conformados, interconectados y las seguridades que posee; por lo tanto en esta investigación se realiza un inventario de los recursos existentes, se los clasifica, se identifican los servicios actuales, se analiza el tráfico de red, con el fin de determinar las posibles causas que se presenten en la congestión de los servicios de la misma y que hacen que la navegación y acceso a los recursos sean lentos; así como también el tratamiento de las medidas de seguridad para los equipos e información. Este Proyecto también incluye una propuesta de solución para mejorar la plataforma tecnológica de red, la distribución de los recursos existentes, identificar los servicios necesarios, determinar la mejor ruta de comunicación de la red, clasificar el tráfico para dotar de calidad de servicio a los procesos de comunicación, así como también una estructura de cómo denominar a los recursos, las seguridades que se deben aplicar para un buen rendimiento, confiabilidad e integridad de la información; se establece también una propuesta de políticas informáticas para el correcto uso de las tecnologías, recursos e información y se explica la conformación de un "Departamento Centralizado de Tecnología de la Información y Comunicación" que se encargue de la administración, planificación, ejecución y evaluación de los procesos informáticos que se ajusten a los proyectos institucionales y provinciales.

ABSTRACT

This project shows an analysis of the current situation of the technology platform and network of information technology services of Honorable Consejo Provincial de Tungurahua and how they are shaped, interconnected and the assurances that they have. So, in this investigation, an inventory of resources they have is carried out. They are classified, existing services are identified and the traffic network is analyzed in order to identify possible cases presented in congestion of network services which make navigation and access to resources slow. Also, a treatment is needed regarding security measures for equipment and information. In addition, this project includes a proposal for settlement for the best technology platform network, distribution of existing resources, identifies the necessary services, determines the best communication network´s route, classifies traffic to provide quality service to the communication process, as well as a structure of how they should call resources and the assuring to be applied for a good performance, reliability and integrity of information. A proposal for information technology policies is also set out for the proper use of technologies, resources and information. It explains the formation of a "Centralized Department of Information Technology and Communication" to be responsible for administration, planning, implementation and evaluation of computing processes, so they adjust to the institutional projects as well the province ones.

TABLA DE CONTENIDOS

FIGURAS

TABLAS

INTRODUCCION

El presente documento muestra las causas por la cual la red del H. Consejo Provincial de Tungurahua presenta dificultades en el tráfico de red originado por la saturación de dispositivos de red conectados dentro de una sola dirección de red, también por la inexistencia de políticas, reglas y funciones que reduzca el nivel tráfico y la carencia de medidas de seguridad y planes de contingencia, debido a la baja valoración de las nuevas Tecnologías de la Información y Comunicación presentando los siguientes problemas: Demora en la transmisión de datos, Reducción del ancho de banda ,Subutilización de recursos informáticos., Riesgo de integridad y confidencialidad de la información, Vulnerabilidad contra ataques externos y el Incremento de costos técnicos y operativos.

Motivo por el cual se hace un recuento de toda la evolución tecnológica que ha experimentado el H. Consejo Provincial de Tungurahua, indicando además la carencia de una Dirección o Departamento de Tecnología de la Información y Comunicación que fortalezca la planificación informática institucional.

Además se hace un análisis de la situación actual de la red, con todo el inventario de dispositivos, servicios, y seguridades que se tienen

actualmente, además de un análisis de tráfico de red para determinar las vulnerabilidades.

Luego de esto, se presenta una propuesta de cómo se debería configurar la red, clasificando el tráfico de las aplicaciones para obtener mejor servicios con calidad conjuntamente con un diseño de seguridades, políticas y distribución de la red, normalización de nombres de equipos; todo esto permitirá reducir el dominio de colisiones y obtener mejores resultados al momento de trabajar en las aplicaciones importantes de la Institución bajo los servicios de la red,

De esta manera se espera obtener una plataforma robusta, óptima, con calidad de servicios y segura que permita trabajar de manera transparente al usuario y que se pueda acoplar a nuevos requerimientos y servicios futuros de la Institución y su desarrollo tecnológico.

CAPÍTULO I

1. PLANTEAMIENTO DEL PROYECTO

1.1. Antecedentes

El Honorable Consejo Provincial de Tungurahua (HCPT), es una institución de derecho público, goza de autonomía y representa a la provincia. Tiene personería jurídica, con capacidad para realizar los actos que fueren necesarios para el cumplimiento de sus fines, en la forma y condiciones que determinan la Constitución y las leyes.

Fundamentalmente, su misión es impulsar el desarrollo cultural y material de la provincia, y colaborar con el Estado y las municipalidades en la respectiva circunscripción, para la realización armónica de los fines nacionales.

Su estructura organizacional se divide en 5 niveles de gestión: Directivo, Ejecutivo; Asesor, Apoyo y Operativo. Dentro del nivel directivo encontramos al Consejo Provincial (Prefecto y Consejeros); el nivel ejecutivo lo conforma la Prefectura; el nivel asesor lo integran las Direcciones de Planificación,

Relaciones externas, y el Departamento Jurídico; el nivel de Apoyo lo conforman las Direcciones Administrativa, Financiera, Secretaria General; dentro de los Niveles de Operativos encontramos a las Direcciones de Vías y Construcciones, Recursos Hídricos y Gestión Ambiental, Producción, y Desarrollo Humano y Cultura.

Es importante señalar que la Unidad de Sistemas Informáticos está bajo la dependencia de la Dirección Administrativa, fungiendo las actividades de Unidad Técnica sobre la tecnología que abarca esta rama.

El H. Consejo Provincial de Tungurahua está conformada por 3 dependencias físicas: El Edificio Principal ubicada en las calles Bolívar y Castillo, El edificio "Centro de Promociones y Servicios" en las Calles Sucre y Castillo y La unidad de Talleres y Bodega del HCPT, ubicada en la Av. Gonzales Suarez y Av. América (Ingahurco).

A partir del año 2002 el Consejo Provincial de Tungurahua comenzó a organizar su infraestructura de red informática estableciendo su topología en estrella con dispositivos de categoría 5 en UTP, y actualmente cuenta además con dispositivos inalámbricos para las Áreas Wireless.

El Consejo Provincial de Tungurahua cuenta con más de 110 computadores todos interconectados en red mediante las diferentes topologías indicadas

La conexión de internet se la cuenta con el proveedor Andinanet en un canal ADSL de 1024/512 kbps, distribuida por un servidor proxy como puerta de enlace. Se cuenta también con el servicio de correo electrónico con el servidor Lotus Domino 7 bajo el dominio tungurahua.gov.ec, estos servidores de Base de Datos y de Internet tienen como sistema operativo Solaris 9. Además posee un Servidor de Dominio con Windows Small Business 2003 Server.

1.2. Definición del problema

El principal problema que presenta la institución en el ámbito informático es **el congestionamiento de los paquetes de información.**

Este problema se origina por dos causas:

- **La limitada e ineficiente distribución física,** originada por la saturación de dispositivos de red, los mismos que se encuentran conectados dentro de una sola dirección, bajo un dominio hcpt.gov.ec y utilizando direcciones IPs fijas lo que conlleva a que se forme **un sólo dominio de broadcast**

- **La ausencia de una estandarización lógica de la infraestructura de red informática**, provocado por la inexistencia de políticas, reglas y funciones que reduzca el nivel tráfico de información en los conmutadores, teniendo que cualquier petición o respuesta a un protocolo de red, se distribuye por toda las 3 infraestructuras del Consejo Provincial de Tungurahua.

Otro de los problemas que se presentan es:

- **La carencia de medidas de seguridad** y planes de contingencia, debido a la baja valoración de las nuevas Tecnologías de la Información y Comunicación

Dentro de los efectos que generan estos problemas se describen los siguientes:

- Demora en la transmisión de datos
- Reducción del ancho de banda
- Subutilización de recursos informáticos.
- Riesgo de integridad y confidencialidad de la información
- Vulnerabilidad contra ataques externos
- Incremento de costos técnicos y operativos

1.3. Hipótesis

La reingeniería de la red informática del H. Consejo Provincial de Tungurahua contribuirá a mejorar la calidad de los servicios informáticos institucionales mediante el control de los siguientes factores claves: velocidad de procesamiento de las peticiones de red, ancho de banda de la red, redistribución de los recursos de red, protocolos de la Calidad de Servicios y planes de seguridad y de contingencias.

1.4. Objetivos

1.4.1. General

Elaborar una propuesta técnica orientada a mejorar la productividad de los recursos de la red informática con calidad de servicios del H. Consejo Provincial de Tungurahua.

1.4.2. Específicos

- Analizar la situación actual de la infraestructura tecnológica del H. Consejo Provincial de Tungurahua que permita obtener a detalle los

diferentes tipos de recursos y servicios existentes a fin de determinar si son necesarios.

- Diseñar una propuesta técnica que se ajuste a los requerimientos institucionales para el fortalecimiento de la red informática del H. Consejo Provincial de Tungurahua orientado a la calidad de los servicios.

- Establecer políticas para la administración y control de tráfico de información de la red informática del H. Consejo Provincial de Tungurahua con la finalidad de proteger la integridad de la información.

1.5. Metodología

1.5.1. Fuentes de investigación

Las fuentes de investigación para el presente proyecto esta divididas en las siguientes entidades:

- Infraestructura del H. Consejo Provincial de Tungurahua
- Empresas similares para comparación
- Universidades y Bibliotecas cercanas a la zona
- Expertos, Asesores y Colaboradores
- Internet y otros

- Documentación como libros de redes informáticas, manuales de configuración

1.5.2. Instrumentos para obtener información

Dentro de las herramientas metodológicas que se utilizarán en la presente investigación se detallan los siguientes:

A nivel fuentes secundarias

En un primer momento, el estudio exploratorio se constituirá en un elemento clave para la obtención de información secundaria.

A nivel de fuentes primarias:

Los instrumentos que se utilizarán para levantar información serán: herramientas tecnológicas y fichas técnicas

1.5.3. Métodos de investigación

Para el análisis y diseño de redes se utilizará como metodología de implementación y revisión los conceptos descritos y utilizados para el diseño de las Redes CISCO, lo cual también se establecerá como prácticas de

mejoramiento continuo de redes y utilizando las siguientes fases: Análisis de red, control y análisis de prestaciones, medidas de prestaciones, Análisis de los enlaces, Diseño de la red, Cálculo de enlaces y nodos, Diseño de la red.

Se utilizará los principios sobre el ciclo de vida de diseño de redes PDIOO (Planificación, Diseño Implementación, Operación y Optimización) así como los esquemas modulares de diseño de redes para el modelo jerárquico y el modelo de redes complejas empresariales de Cisco (Cisco Enterprise Composite Network)

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Redes de Datos

2.1.1. La red informática en el siglo 21

Hoy en día el avance de las tecnologías de la comunicación permite interconectar redes a grandes distancias con lo que se puede compartir información, recursos y servicios, permitiendo optimizar y automatizar varios de los procesos que antes se tardaban mucho en realizar.

Las redes de datos se desarrollaron como consecuencia de aplicaciones comerciales diseñadas para microcomputadores. Por aquel entonces, los microcomputadores no estaban conectados entre sí como sí lo estaban las terminales de computadores mainframe, por lo cual no había una manera eficaz de compartir datos entre varios computadores.

Se tornó evidente que el uso de disquetes para compartir datos no era un método eficaz ni económico para desarrollar la actividad empresarial. La red

a pie creaba copias múltiples de los datos. Cada vez que se modificaba un archivo, había que volver a compartirlo con el resto de sus usuarios. Si dos usuarios modificaban el archivo, y luego intentaban compartirlo, se perdía alguno de los dos conjuntos de modificaciones. Las empresas necesitaban una solución que resolviera con éxito los tres problemas siguientes:

- Cómo evitar la duplicación de equipos informáticos y de otros recursos
- Cómo comunicarse con eficiencia
- Cómo configurar y administrar una red

Las empresas se dieron cuenta de que la tecnología de networking podía aumentar la productividad y ahorrar gastos. Las redes se agrandaron y extendieron casi con la misma rapidez con la que se lanzaban nuevas tecnologías y productos de red.

A principios de la década de 1980 networking se expandió enormemente, aun cuando en sus inicios su desarrollo fue desorganizado.

2.1.2. Importancia de la red informática en las empresas publicas

La red informática es el eje principal para el desarrollo informático de los procesos internos que se generan en toda entidad, permitiendo compartir informes, documentos y hacer un seguimiento de los trámites y solicitudes. La conectividad física permitió un aumento en la productividad permitiendo que se compartan impresoras, servidores y software. Los sistemas tradicionales de red requieren que las estaciones de trabajo permanezcan estacionarias permitiendo movimientos sólo dentro del alcance de los medios y del área de la oficina.

2.1.3. Dispositivos de red

Los equipos que se conectan de forma directa a un segmento de red se denominan dispositivos. Estos dispositivos se clasifican en dos grandes grupos.

El primer grupo está compuesto por los dispositivos de usuario final; éstos incluyen los computadores, impresoras, escáneres, y demás dispositivos que brindan servicios directamente al usuario.

El segundo grupo está formado por los dispositivos de red. Los dispositivos de red son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

Figura 1: Dispositivos de usuario final

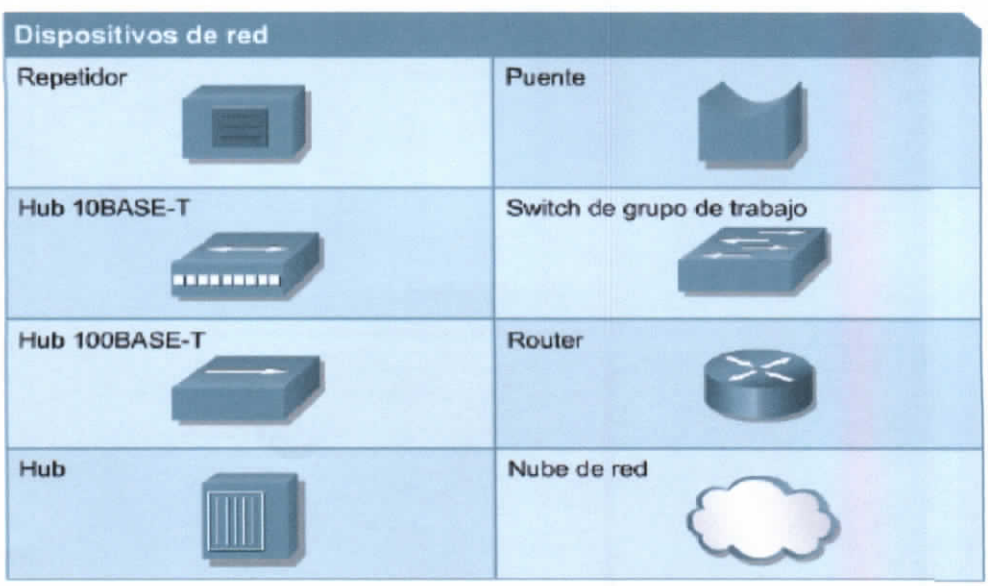


Figura 2: Dispositivos de red

2.1.4. Topologías de red

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos.

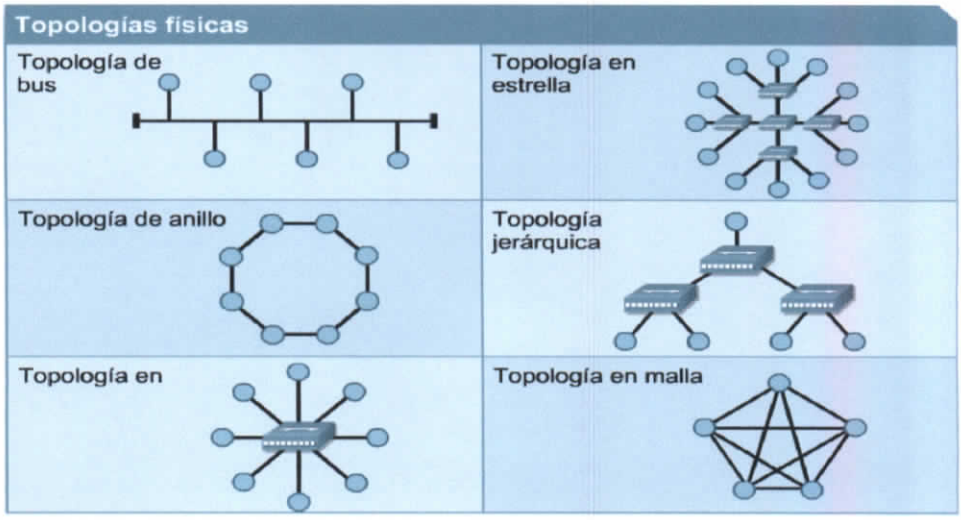


Figura 3: Topologías de red

- Una topología de bus usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.

- La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.

- La topología en estrella conecta todos los cables con un punto central de concentración.

- Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.

- Una topología jerárquica es similar a una estrella extendida. Pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.

- La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. Como se puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Aunque la Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.

2.1.5. Protocolos

Los conjuntos de protocolos son colecciones de protocolos que posibilitan la comunicación de red desde un host, a través de la red, hacia otro host. Un protocolo es una descripción formal de un conjunto de reglas y convenciones

que rigen un aspecto particular de cómo los dispositivos de una red se comunican entre sí. Los protocolos determinan el formato, la sincronización, la secuenciación y el control de errores en la comunicación de datos. Sin protocolos, el computador no puede armar o reconstruir el formato original del flujo de bits entrantes desde otro computador

2.1.6. Red de área local LAN

Las LAN permiten a las empresas aplicar tecnología informática para compartir localmente archivos e impresoras de manera eficiente, y posibilitar las comunicaciones internas. Un buen ejemplo de esta tecnología es el correo electrónico. Los que hacen es conectar los datos, las comunicaciones locales y los equipos informáticos.

Algunas de las tecnologías comunes de LAN son:

- Ethernet
- Token Ring
- FDDI

2.1.7. Redes de área amplia (WAN)

Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares.

Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes.

Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas personalmente. Networking de área amplia también dio lugar a una nueva clase de trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar. Algunas de las tecnologías comunes de WAN son:

- Módems
- Red digital de servicios integrados (RDSI)
- Línea de suscripción digital (DSL - Digital Subscriber Line)
- Frame Relay
- Series de portadoras para EE.UU. (T) y Europa (E): T1, E1, T3, E3
- Red óptica síncrona (SONET)

2.1.8. Red de área metropolitana

Es una red de alta velocidad (banda ancha) que dando cobertura en una área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE), la tecnología de pares de cobre se posiciona como una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades que van desde los 2Mbps y los 155Mbps.

2.1.9. Redes virtuales Privadas (VPN)

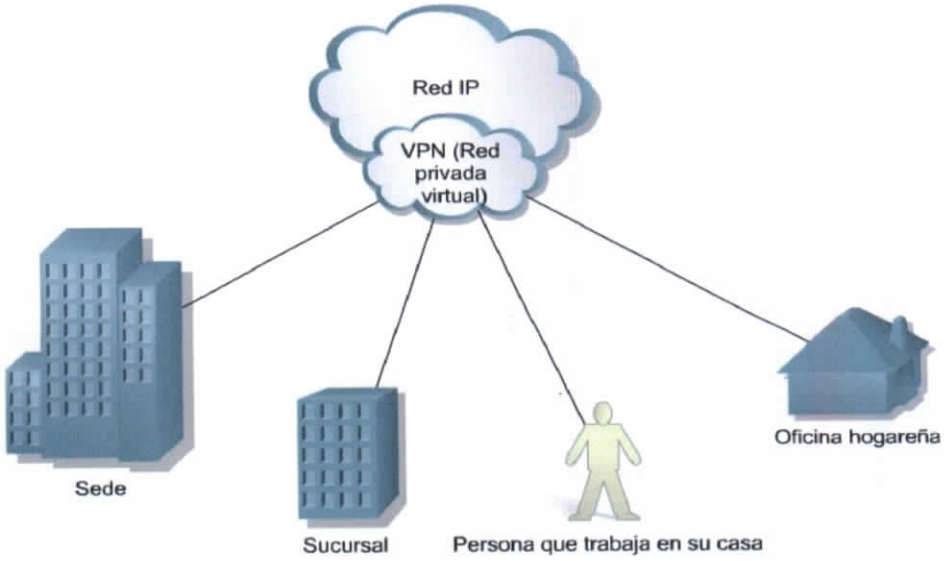


Figura 4: Ejemplo de redes virtuales privadas

Una VPN es una red privada que se construye dentro de una infraestructura de red pública, como la Internet global. Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un Router VPN en la sede.

2.1.10. Modelo OSI

Fue creado por la ISO (Organización Estándar Internacional) y en él pueden modelarse o referenciarse diversos dispositivos que reglamenta la ITU (Unión de Telecomunicación Internacional), con el fin de poner orden entre todos los sistemas y componentes requeridos en la transmisión de datos, además de simplificar la interrelación entre fabricantes. Así, todo dispositivo de cómputo y telecomunicaciones podrá ser referenciado al modelo y por ende concebido como parte de un sistema interdependiente con características muy precisas en cada nivel.

El Modelo OSI cuenta con 7 capas o niveles:

Figura 5: Capas del Modelo OSI

Capa de Aplicación: Procesos de red a aplicaciones.

Suministra servicios de red a los procesos de aplicaciones (como, por ejemplo, correo electrónico, transferencia de archivos y emulación de terminarles)

Capa de Presentación: Representación de datos

Garantizar que los datos sean legibles para el sistema receptor, se encarga del formato y la estructura de los datos, negocia la sintaxis de transferencia de datos para la capa de aplicación

Capa de Sesión: Comunicación entre hosts

Establece, administra y termina sesiones entre aplicaciones

Capa de Transporte: Conexiones de extremo a extremo

Se ocupa de aspectos de transporte entre hots, confiabilidad del transporte de datos, establecer, mantener, terminar circuitos virtuales, detección de fallas y control de flujo de información de recuperación

Capa de Red: Dirección de red y determinación de mejor ruta

Provee transferencia confiable de datos a través de los medios, conectividad y selección de ruta entre sistemas

Capa de Enlace de Datos: Control director de enlaces, acceso a los medios

Provee transferencia confiable de datos a través de los medios, conectividad y selección de ruta entre sistemas, Direccionamiento lógico, entrega de mejor esfuerzo.

Capa Físico: Transmisión binaria

Cables, conectores, voltajes, velocidades de transmisión de datos

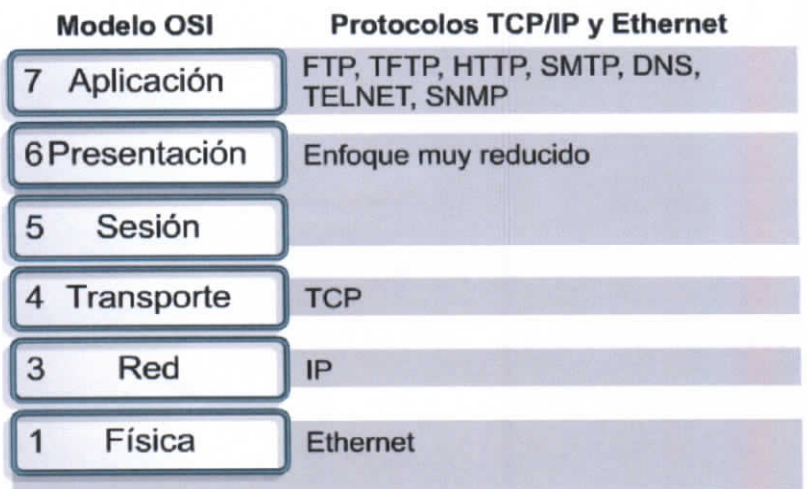


Figura 6: Protocolos del Modelo OSI

2.2. Medios de comunicación

El cable de cobre se utiliza en casi todas las LAN. Hay varios tipos de cable de cobre disponibles en el mercado, y cada uno presenta ventajas y desventajas. La correcta selección del cableado es fundamental para que la red funcione de manera eficiente. Debido a que el cobre transporta información utilizando corriente eléctrica, es importante comprender algunos principios básicos de la electricidad a la hora de planear e instalar una red.

La fibra óptica es el medio utilizado con mayor frecuencia en las transmisiones de punto a punto de mayor distancia y alto ancho de banda que requieren los backbones de LAN y las WAN. En los medios ópticos, se utiliza la luz para transmitir datos a través de una delgada fibra de vidrio o de plástico. Las señales eléctricas hacen que el transmisor de fibra óptica genere señales luminosas que son enviadas por la fibra. El host receptor recibe las señales luminosas y las convierte en señales eléctricas en el extremo opuesto de la fibra. Sin embargo, no hay electricidad en el cable de fibra óptica en sí. De hecho, el vidrio utilizado es un muy buen aislante eléctrico.

La introducción de la tecnología inalámbrica elimina estas limitaciones y otorga portabilidad real al mundo de la computación. En la actualidad, la tecnología inalámbrica no ofrece las transferencias a alta velocidad, la

seguridad o la confiabilidad de tiempo de actividad que brindan las redes que usan cables. Sin embargo, la flexibilidad de no tener cables justifica el sacrificio de estas características.

2.2.1 Cable coaxial

El cable coaxial consiste en un conductor de cobre rodeado de una capa de aislante flexible. El conductor central también puede ser hecho de un cable de aluminio cubierto de estaño que permite que el cable sea fabricado de forma económica. Sobre este material aislante existe una malla de cobre tejida u hoja metálica que actúa como el segundo hilo del circuito y como un blindaje para el conductor interno. Esta segunda capa, o blindaje, también reduce la cantidad de interferencia electromagnética externa. Cubriendo la pantalla está la chaqueta del cable.

Figura 7: Cable Coaxial

2.2.2. Cable STP

El cable de par trenzado blindado (STP) combina las técnicas de blindaje, cancelación y trenzado de cables. Cada par de hilos está envuelto en un papel metálico. Los dos pares de hilos están envueltos juntos en una trenza o papel metálico. Generalmente es un cable de 150 ohmios. Según se especifica para el uso en instalaciones de redes Token Ring, el STP reduce el ruido eléctrico dentro del cable como, por ejemplo, el acoplamiento de par a par y la diafonía. El STP también reduce el ruido electrónico desde el exterior del cable, como, por ejemplo, la interferencia electromagnética (EMI) y la interferencia de radiofrecuencia (RFI).

El cable de par trenzado blindado comparte muchas de las ventajas y desventajas del cable de par trenzado no blindado (UTP). El cable STP brinda mayor protección ante toda clase de interferencias externas, pero es más caro y de instalación más difícil que el UTP.

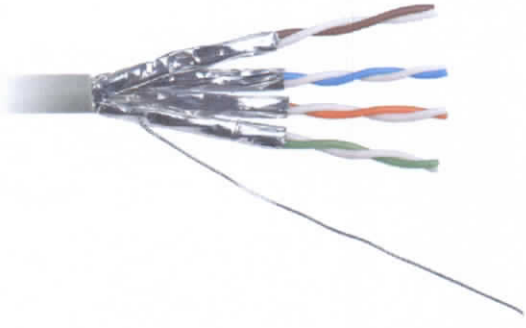


Figura 8: Cable STP

2.2.3. Cable UTP

El cable de par trenzado no blindado (UTP) es un medio de cuatro pares de hilos que se utiliza en diversos tipos de redes. Cada uno de los 8 hilos de cobre individuales del cable UTP está revestido de un material aislante. Además, cada par de hilos está trenzado. Este tipo de cable cuenta sólo con el efecto de cancelación que producen los pares trenzados de hilos para limitar la degradación de la señal que causan la EMI y la RFI. Para reducir aún más la diafonía entre los pares en el cable UTP, la cantidad de trenzados en los pares de hilos varía. Al igual que el cable STP, el cable UTP debe seguir especificaciones precisas con respecto a cuánto trenzado se permite por unidad de longitud del cable.

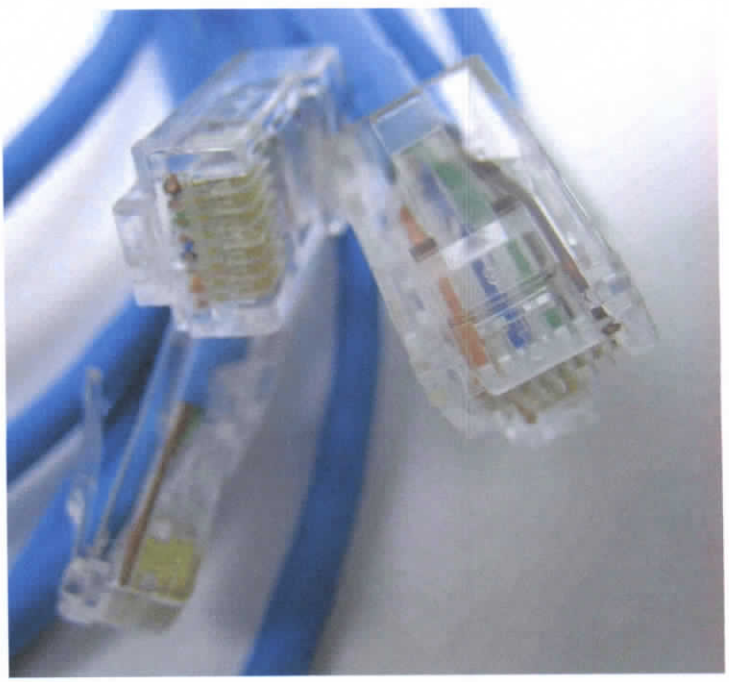


Figura 9: Cable UTP

2.2.4. Fibra óptica

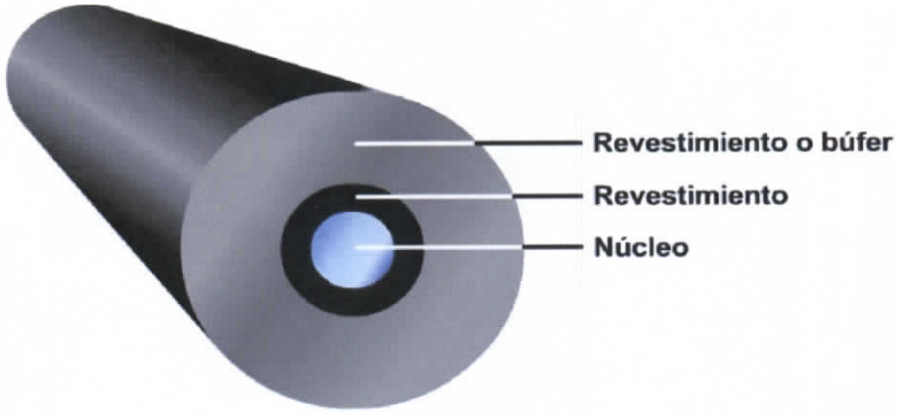


Figura 10: Fibra óptica

Multimodo

La parte de una fibra óptica por la que viajan los rayos de luz recibe el nombre de núcleo de la fibra. Los rayos de luz sólo pueden ingresar al núcleo si el ángulo está comprendido en la apertura numérica de la fibra. Asimismo, una vez que los rayos han ingresado al núcleo de la fibra, hay un número limitado de recorridos ópticos que puede seguir un rayo de luz a través de ésta. Estos recorridos ópticos reciben el nombre de modos. Si el diámetro del núcleo de la fibra es lo suficientemente grande como para permitir varios trayectos que la luz pueda recorrer a lo largo de la fibra, esta fibra recibe el nombre de fibra "multimodo". La fibra monomodo tiene un núcleo mucho más pequeño que permite que los rayos de luz viajen a través de la fibra por un sólo modo.

Monomodo

La fibra monomodo consta de las mismas partes que una multimodo. El revestimiento exterior de la fibra monomodo es, en general, de color amarillo. La mayor diferencia entre esta fibra y la multimodo es que la primera permite que un solo modo de luz se propague a través del núcleo de menor diámetro de la fibra óptica. El núcleo de una fibra monomodo tiene de ocho a diez micrones de diámetro. Los más comunes son los núcleos de nueve micrones.

2.2.5. Dispositivos inalámbricos

Una red inalámbrica puede constar de tan sólo dos dispositivos. - Los nodos pueden ser simples estaciones de trabajo de escritorio o computadores de mano. Equipada con NIC inalámbricas, se puede establecer una red 'ad hoc' comparable a una red cableada de par a par. Ambos dispositivos funcionan como servidores y clientes en este entorno. Aunque brinda conectividad, la seguridad es mínima, al igual que la tasa de transferencia.

Figura 11: Medios Inalámbricos

2.3. Ethernet

Ethernet es ahora la tecnología LAN dominante en el mundo. Ethernet no es una tecnología sino una familia de tecnologías LAN que se pueden entender mejor utilizando el modelo de referencia OSI. Todas las LAN deben afrontar el tema básico de cómo denominar a las estaciones individuales (nodos) y Ethernet no es la excepción. Las especificaciones de Ethernet admiten diferentes medios, anchos de banda y demás variaciones de la Capa 1 y 2. Sin embargo, el formato de trama básico y el esquema de direccionamiento es igual para todas las variedades de Ethernet.

Para que varias estaciones accedan a los medios físicos y a otros dispositivos de networking, se han inventado diversas estrategias para el control de acceso a los medios. Comprender la manera en que los dispositivos de red ganan acceso a los medios es esencial para comprender y detectar las fallas en el funcionamiento de toda la red.

Ethernet no es una tecnología para networking, sino una familia de tecnologías para networking que incluye Legacy, Fast Ethernet y Gigabit Ethernet. Las velocidades de Ethernet pueden ser de 10, 100, 1000 ó 10000 Mbps. El formato básico de la trama y las subcapas del IEEE de las Capas OSI 1 y 2 siguen siendo los mismos para todas las formas de Ethernet.

Velocidad	Método de señalización	Medio
10	BASE	2
100	BROAD	5
1000		-T
10G		-TX
		-SX
		-LX

Figura 12: Clasificación de Ethernet

La descripción abreviada consta de:

- Un número que indica el número de Mbps que se transmiten.
- La palabra "base", que indica que se utiliza la señalización banda base.
- Una o más letras del alfabeto que indican el tipo de medio utilizado (F = cable de fibra óptica, T =par trenzado de cobre no blindado).

Ethernet emplea señalización banda base, la cual utiliza todo el ancho de banda del medio de transmisión. La señal de datos se transmite directamente por el medio de transmisión. Ethernet utiliza la señalización

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbps	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100Mbps	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex(hub) y Full Duplex(switch)
100BaseTX	100Mbps	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex(hub) y Full Duplex(switch)
100BaseFX	100Mbps	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000Mbps	4 pares trenzado (categoría 5UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1000Mbps	Fibra óptica (multimodo)	550 m	Estrella. Full Duplex (switch)
1000BaseLX	1000Mbps	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex (switch)

Tabla 1: Tecnologías Ethernet

2.4. Conmutación – Switching

Ethernet compartida funciona muy bien en circunstancias ideales. Cuando el número de dispositivos que intentan acceder a la red es bajo, el número de colisiones permanece dentro de los límites aceptables. Sin embargo, cuando el número de usuarios de la red aumenta, el mayor número de colisiones puede causar que el rendimiento sea intolerablemente malo. El puenteo se desarrolló para aliviar los problemas de rendimiento que surgieron con el aumento de las colisiones. La conmutación surgió del puenteo y se ha convertido en la tecnología clave de las LAN modernas de Ethernet.

Las colisiones y broadcasts son sucesos esperados en la networking moderna. Ellas, de hecho, están planeadas dentro del diseño de Ethernet y de las tecnologías de capa avanzadas. Sin embargo, cuando las colisiones y broadcasts ocurren en un número que se encuentra por encima del óptimo, el rendimiento de la red se ve afectado. El concepto de dominios de colisión y de broadcast trata las formas en que pueden diseñarse las redes para limitar los efectos negativos de las colisiones y broadcasts. Este módulo explora los efectos de las colisiones y broadcasts sobre el tráfico de red y luego describe cómo se utilizan los puentes y routers para segmentar las redes y mejorar el rendimiento.

2.4.1. Dominios de colisión

Los dominios de colisión son los segmentos de red física conectados, donde pueden ocurrir colisiones. Las colisiones causan que la red sea ineficiente. Cada vez que ocurre una colisión en la red, se detienen todas las transmisiones por un período. La duración de este período sin transmisión varía y depende de un algoritmo de postergación para cada dispositivo de la red.

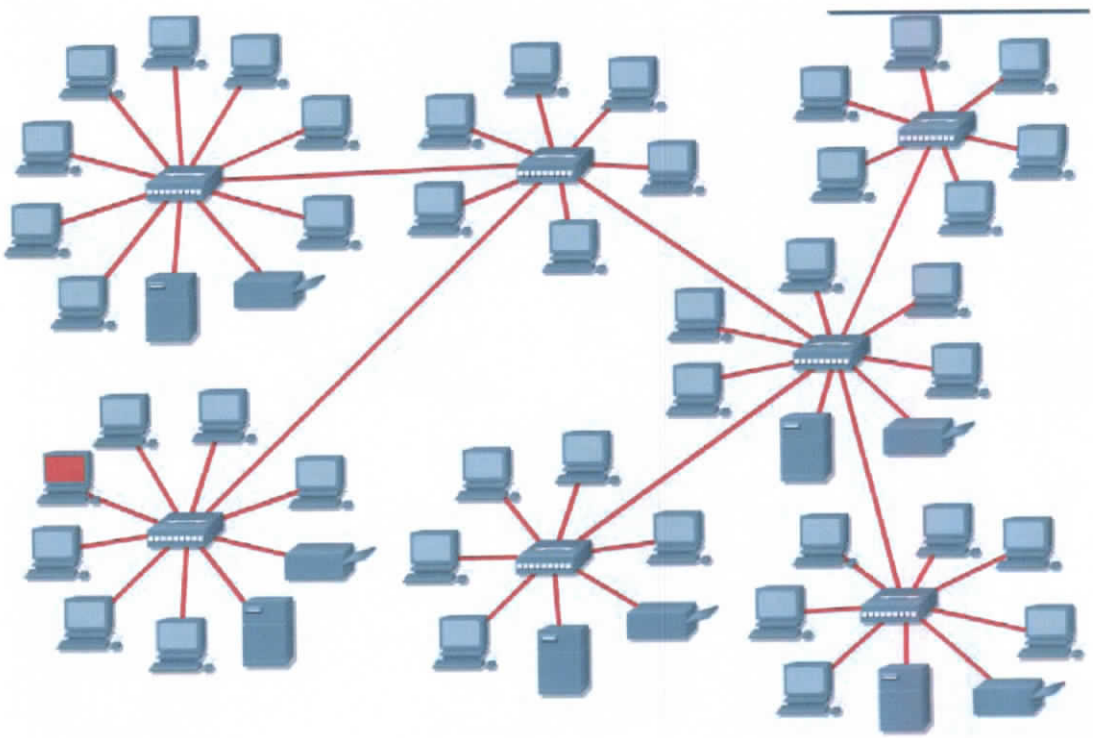
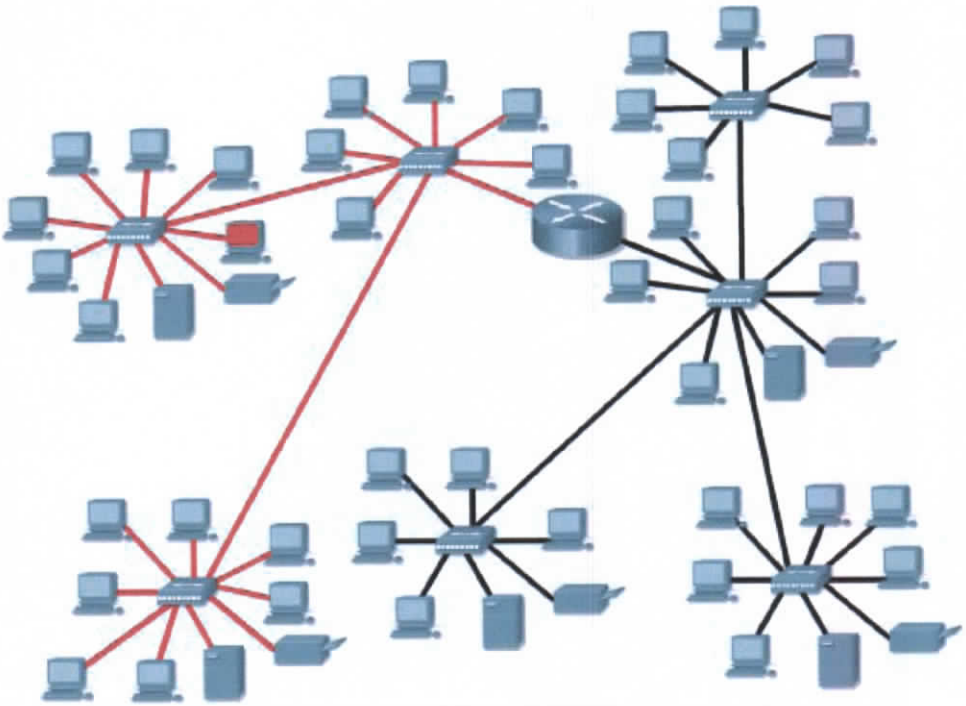


Figura 13: Ejemplo de dominio de colisión

2.4.2. Dominios de broadcast

Un dominio de broadcast es un grupo de dominios de colisión conectados por dos dispositivos de Capa 2. Dividir una LAN en varios dominios de colisión aumenta la posibilidad de que cada host de la red tenga acceso a los medios. Efectivamente, esto reduce la posibilidad de colisiones y aumenta el ancho de banda disponible para cada host. Pero los dispositivos de Capa 2 envían broadcasts, y si son excesivos, pueden reducir la eficiencia de toda la LAN. Los broadcasts deben controlarse en la Capa 3, ya que los dispositivos de Capa 1 y Capa 2 no pueden hacerlo. El tamaño total del dominio del broadcast puede identificarse al observar todos los dominios de colisión que procesan la misma trama de broadcast.

En otras palabras, todos los nodos que forman parte de ese segmento de red delimitados por un dispositivo de Capa 3. Los dominios de broadcast están controlados en la Capa 3 porque los routers no envían broadcasts. Los routers, en realidad, funcionan en las Capas 1, 2 y 3. Ellos, al igual que los dispositivos de Capa 1, poseen una conexión física y transmiten datos a los medios. Ellos tienen una encapsulamiento de Capa 2 en todas las interfaces y se comportan como cualquier otro dispositivo de Capa 2. Es la Capa 3 la que permite que el router segmente dominios de broadcast.



Se contiene un broadcast de capa 2 mediante el uso de un router en lugar de un dispositivo de puenteo. Los dispositivos de Capa 3 son los únicos que contienen broadcasts.

Figura 14: Ejemplo Dominio de Broadcast

2.5. Enrutamiento

El Protocolo de Internet (IP) es el principal protocolo de Internet. El direccionamiento IP permite que los paquetes sean enrutados desde el origen al destino usando la mejor ruta disponible. La propagación de paquetes, los cambios en el encapsulamiento y los protocolos que están orientados a conexión y los que no lo están también son fundamentales para asegurar que los datos se transmitan correctamente a su destino.

No existen dos organizaciones idénticas en el mundo. En realidad, no todas las organizaciones pueden adaptarse al sistema de tres clases de direcciones A, B y C. Sin embargo, hay flexibilidad en el sistema de direccionamiento de clases. Esto se denomina división en subredes. La división en subredes permite que los administradores de red determinen el tamaño de las partes de la red con las que ellos trabajan. Después de determinar cómo segmentar su red, ellos pueden utilizar la máscara de subred para establecer en qué parte de la red se encuentra cada dispositivo.

2.6. Redundancia Protocolo Spanning tree

La redundancia en una red es fundamental. Permite que las redes sean tolerantes a las fallas. Las topologías redundantes proporcionan protección contra el tiempo de inactividad, o no disponibilidad, de la red El tiempo de inactividad puede deberse a la falla de un solo enlace, puerto o dispositivo de red. Los ingenieros de red a menudo deben equilibrar el costo de la redundancia con la necesidad de disponibilidad de la red.

Las topologías redundantes basadas en switches y puentes son susceptibles a las tormentas de broadcast, transmisiones de múltiples tramas e inestabilidad de la base de datos de direcciones MAC: Estos problemas pueden inutilizar la red Por lo tanto, la redundancia se debe planificar y supervisar cuidadosamente. Las redes conmutadas brindan las ventajas de

dominios de colisión más pequeños, microsegmentación y operación full duplex. Las redes conmutadas brindan un mejor rendimiento.

La redundancia en una red es necesaria para protegerla contra la pérdida de conectividad debido a la falla de un componente individual. Sin embargo, esta medida puede dar como resultado topologías físicas con loops. Los loops de la capa física pueden causar problemas graves en las redes conmutadas.

El protocolo Spanning-Tree se usa en redes conmutadas para crear una topología lógica sin loops a partir de una topología física con loops. Los enlaces, puertos y switches que no forman parte de la topología activa sin loops no envían tramas de datos. El protocolo Spanning Tree es una herramienta poderosa que les otorga a los administradores de red la seguridad de contar con una topología redundante sin que exista el riesgo de que se produzcan problemas provocados por los loops de conmutación.

2.7. Seguridad de redes

Actualmente se están desarrollando aplicaciones, sistemas y protocolos que ayuden a proteger la integridad de la información y sean más confiables, mediante la aplicación de normas, políticas de seguridad para que las

aplicaciones resulten ser lo más seguras de utilizar, tales como contraseñas cifradas, firmas digitales y codificación de la información, que han permitido proporcionar cierto grado de seguridad y confidencialidad de nuestra información contra amenazas informáticas y prevenir el hurto de información, suplantación de identidad, estafas y robos de dinero de cuentas bancarias y tarjetas de crédito.

2.8. Metodología de Diseño de Redes

Cisco ha desarrollado una metodología del ciclo de vida del diseño de redes, en las cuales se tienen 6 fases PDIOO como Planificación, Diseño, Implementación, Operatividad, Optimización, y Retiramiento.

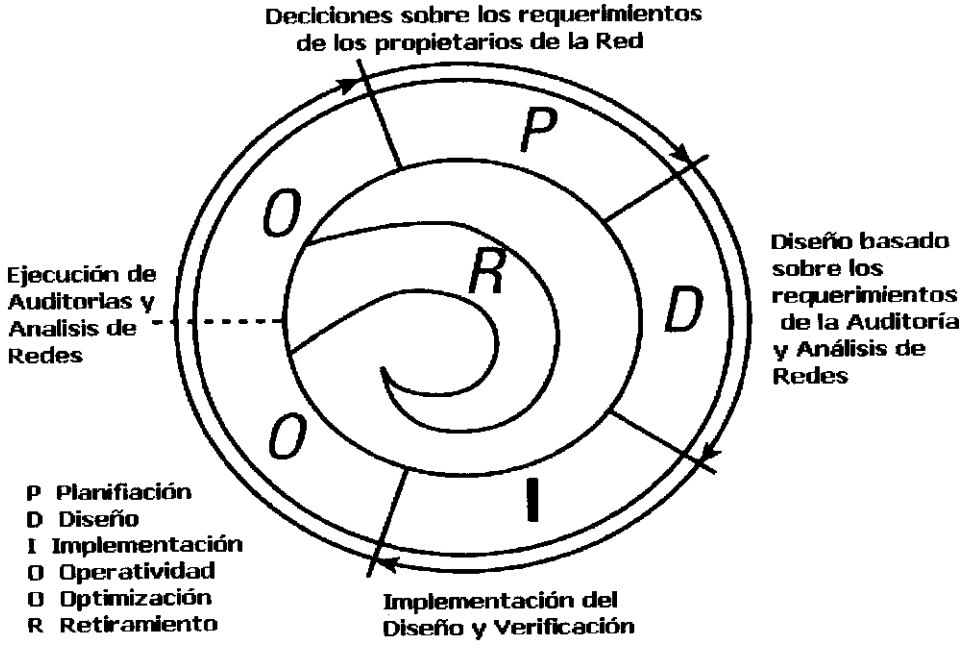


Figura 15: Ciclo de vida de las redes

El diseño de redes debe contemplar las siguientes tareas:

- La determinación de requerimientos
- El Análisis de la red existente en el caso de haber una
- La preparación preliminar del diseño
- La Instalación de la red
- El Monitoreo y rediseño si es necesario
- La Documentación de Mantenimiento

2.9. Diseño Modular de Redes

Es un modelo de diseño de redes el cual se divide en grupos o bloques de diferente tamaño dependiendo de las funciones que estos realizan, con el objetivo de reducir esfuerzos de tiempos y diseño.

Estos Modelos pueden ser Jerárquicos en los que intervienes tres funciones o capas como Acceso, Distribución y Núcleo.

También está el modelo de Redes Complejas Empresarial de Cisco (Cisco Enterprise Composite Network) el cual fue desarrollado para abarcar redes más grandes y que están en diferentes infraestructuras, dentro de las funcionalidades de esta tenemos: El Campus Empresarial, Tecnología de Punta y el Proveedor de Servicios de Alta Tecnología.

2.10. Calidad de Servicios (QoS)

En primer lugar, nos introduciremos en lo que es QoS y porque es un servicio importante a las redes de hoy. Las necesidades relacionadas con la QoS de diversos tipos de tráfico se describen a continuación.

Dos modelos para el despliegue de extremo a extremo en la QoS en una red se examinan a continuación: Servicios Integrados (IntServ) y servicios diferenciados (DiffServ). QoS herramientas, incluida la clasificación y el marcado, las politicas y el modelado, evitar la congestión, gestión de la congestión, y el vínculo de herramientas específicas son explicados.

Las características de QoS automática de Cisco (AutoQoS) de routers y conmutadores son introducidos, lo que proporciona una herramienta simple, de forma automática para permitir configuraciones de QoS en conformidad con las recomendaciones de las mejores prácticas de Cisco. Concluimos con algunas consideraciones de diseño de QoS.

Demora, también llamada latencia, es el tiempo que toman los paquetes en transitar a través de la red. La demora tiene dos componentes: fijos y variables. Estos términos se describen de la siguiente manera:

2.10.1. Demoras fijas

Son previsibles retrasos asociados con la preparación y la encapsulación de los datos, que se transmiten en el cable, y el tener que viajar al receptor. Las demoras fijas pueden ser provocadas según las siguientes categorías:

- Demora de Transformación o empaquetamiento, El tiempo que toma para crear los datos que serán enviados. Por ejemplo, para el tráfico de voz, la voz analógica debe ser analizada, convertida a datos digitales y, a continuación, encapsulada en paquetes.
- La demora en la codificación, tiempo que se tarda en transmitir los datos en el alambre. Este retraso está relacionado con la velocidad del enlace físico.
- La demora de propagación tiempo que toman los datos al transitar por la red. En la mayoría de los casos, la demora de propagación es lo suficientemente pequeña por lo que puede ser ignorada.

2.10.2. Demoras variables

Son impredecibles retrasos que resultan de un paquete que espera por el resto del tráfico que está en la cola de la interfaz que será enviada. A medida que más y más grandes paquetes se están enviando, estos retrasos aumentan, ya que la cola empieza a crecer y tiene que esperar el turno

2.10.3. Fluctuación

Es la variación en el retraso experimentado por los paquetes en la red. En el ejemplo de la fluctuación ilustrado en la Figura 6-1, el remitente envía los datos a cabo en intervalos de tiempo coherente, Δt.

El receptor está observando una variación en el retraso de algunos paquetes recibidos que son mayores a Δt mientras que otros son menores de Δt.

La fluctuación por lo general no es perceptible para aplicaciones como transferencia de archivos. Sin embargo, las aplicaciones tales como voz son sensibles a las diferencias en las demoras de los paquetes por ejemplo, un oyente puede escuchar pausas de silencio en donde no deberían existir.

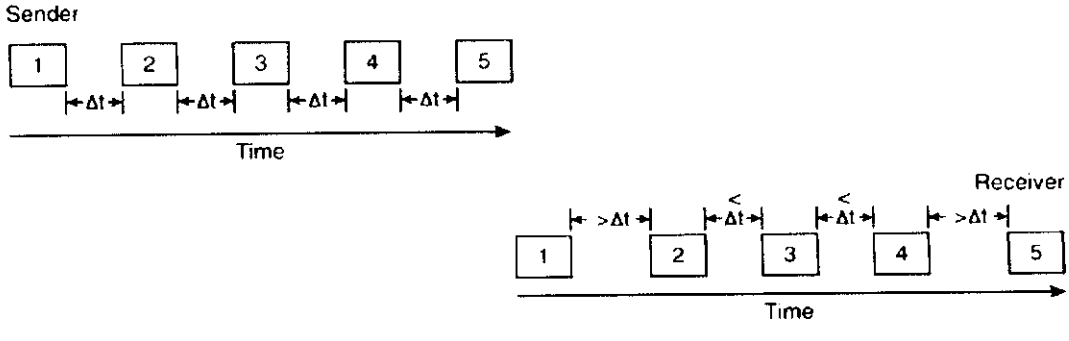


Figura 16: Ejemplo de Fluctuación

2.10.4. Ventajas

QoS le permite controlar y predecir el servicio prestado por su red para una variedad de aplicaciones. La aplicación de QoS tiene muchas ventajas, entre ellas las siguientes: Controlar cuales recursos de la red (ancho de banda, equipos, instalaciones de un área amplia, etc.) están siendo utilizados

- La garantía de que sus recursos se utilicen de forma eficiente de la aplicación de misión crítica, aquellos que son más importantes para su negocio y el que se adquieran otras aplicaciones de servicios sin interferir en este tráfico de misión crítica
- Creación de una base sólida para una completa integración de redes convergentes en el futuro.

2.10.5. Requisitos para QoS de voz, datos, vídeo y otros tráficos

Tráfico de voz, es sensible a los retrasos; retrasos en la variación (fluctuación) y pérdida de paquetes. Las directrices para garantizar la calidad de voz aceptable son los siguientes:

- La demora de una vía no debe ser más de 150 milisegundos (ms).
- La fluctuación no debe ser más de 30 ms.
- No más del 1 por ciento de los paquetes deben perderse.

El ancho de banda requerido para tráfico de voz varía con el algoritmo que comprime el tráfico y en el encapsulado específico de la trama de la capa 2. El tráfico de codificación de llamadas requiere al menos 150 bps (no incluidos los gastos generales de capa 2), en función de los protocolos utilizados.

El vídeo interactivo, o las videoconferencias, tienen el mismo retraso, fluctuación, pérdida de paquetes y requerimientos como el tráfico de voz. La diferencia es el ancho de banda del requerimiento de paquetes de voz que son pequeños mientras los de videoconferencia tienen tamaños de paquetes que pueden variar, así como la velocidad de transmisión de datos. Una orientación general para los gastos generales es proporcionar un adicional de 20 por ciento más que el ancho de banda requerido por los datos.

El vídeo simultáneo tiene diferentes requisitos que el vídeo interactivo. Un ejemplo del uso de video simultáneo es cuando un empleado mira un video en línea durante una sesión de e-learning. Como tal, este flujo de vídeo no es tan sensible a la demora o pérdida como el vídeo interactivo, este requerimiento para el vídeo continuo incluye una pérdida de no más de 5 por ciento y un retraso de no más de 4 a 5 segundos. Dependiendo de la importancia que tiene para la organización, este tráfico se le puede dar preferencia sobre el resto del tráfico.

Tráfico relacionado con el funcionamiento de la red en sí misma también deben ser tomada en cuenta. Un ejemplo de este tipo de tráfico es el protocolo de enrutamiento de mensajes, el tamaño y la frecuencia de estos mensajes varían, dependiendo del protocolo específico utilizado y la estabilidad de la red. La Administración de la Red de datos es otro ejemplo, con inclusión de Simple Network Management Protocol (SNMP) el tráfico entre dispositivos de red y la gestión de la red.

2.10.6. Modelos de QoS

Existen dos modelos para la QoS de despliegue de extremo a extremo en una red de tráfico que no es conveniente para el servicio de mejor esfuerzo: IntServ y DiffServ. QoS de extremo a extremo significa que la red proporciona el nivel de servicio requerido por el tráfico en toda la red, desde un extremo al otro.

Con IntServ, una aplicación solicita los servicios de la red, y los dispositivos de red confirmar que puedan satisfacer la petición, antes de que los datos sean enviados. Los datos de la solicitud se consideran como un flujo de paquetes.

Por el contrario, con DiffServ, cada paquete está marcado, ya que entra en la red sobre la base del tipo de tráfico que contiene. Los dispositivos de red entonces utilizan estas marcas para determinar cómo manejar el paquete que viaja a través de ésta.

2.10.6.1. IntServ

IntServ utiliza un mecanismo explícito de señalización de aplicaciones para dispositivos de red. La solicitud pide un determinado nivel de servicio, incluidas, por ejemplo, su ancho de banda y requisitos de demora. Después que los dispositivos de red han confirmado que pueden cumplir estos requisitos, la aplicación asume a sólo enviar los datos que exige este nivel de servicio.

Aplicaciones en un entorno IntServ utilizan el Protocolo de reserva de recursos (RSVP) para indicar sus necesidades a los dispositivos de red. Los dispositivos de red mantienen la información sobre el flujo de paquetes, y garantizan que el flujo reciba los recursos que necesita mediante el uso apropiado de colas (priorización de tráfico) y métodos de políticas (selectivamente descarta otros paquetes). Dos tipos de servicios prestados en un ambiente IntServ son los siguientes:

- **Tasa de Garantía de Servicio,** Este servicio permite a las aplicaciones reservar el ancho de banda para satisfacer sus necesidades. La red utiliza colas equitativas ponderadas (WFQ) con RSVP para proporcionar este servicio.

- **Servicio de carga controlada,** Este servicio permite a las aplicaciones solicitar bajas demoras y de alto rendimiento, incluso durante los momentos de congestión. La red utiliza RSVP con detección temprana ponderada al azar (WRED) para proporcionar este tipo de servicio.

Porque IntServ requiere RSVP en todos los dispositivos de red, en este momento no es utilizado tanto como DiffServ.

2.10.6.2 DiffServ

Una aplicación en un entorno DiffServ no tiene una explícita señal de la red antes de enviar los datos. En lugar de ello, la red intenta ofrecer un determinado nivel de servicio basado en la QoS especificada en la cabecera de cada paquete. Los dispositivos de red, por lo general en el borde de la red, están configurados para clasificar y marcar los paquetes de acuerdo a su origen, el destino, o el tipo de tráfico en ellas. Dispositivos dentro de la red luego proporcionan los recursos adecuados sobre la base de este marcado. Por ejemplo, los paquetes que contienen el tráfico de voz se

suelen dar mayor prioridad que la transferencia de archivos de datos, debido a las necesidades únicas de voz.

2.10.7. Herramientas de QoS

Algunas de las diversas herramientas que implementan QoS se describen en esta sección y se muestra en el siguiente gráfico

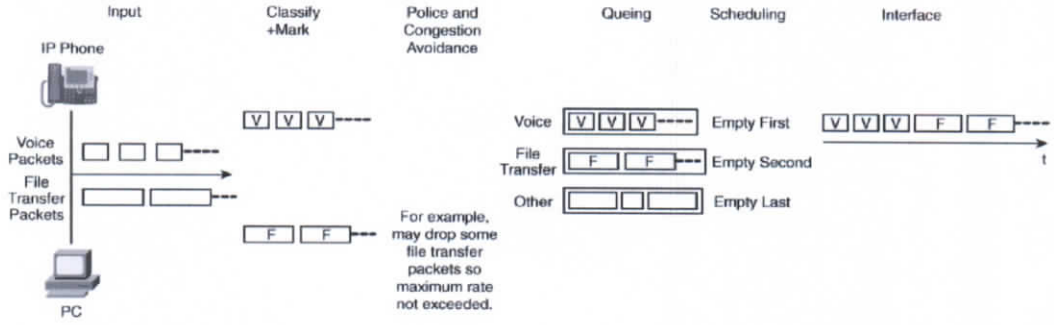


Figura 17: Herramientas de gestión de QoS

Muchos dispositivos de envío de datos en una red. En el ejemplo se muestra en la Figura 17, un teléfono IP produce paquetes que contienen el tráfico de voz, y un PC envía la transferencia de archivos de datos. Como los datos entran en la red, éstos se analizan y clasifican de acuerdo a la forma en que deben tratarse en la red. Después se clasifica, los datos son marcados en consecuencia.

La clasificación y marcado es la base para el resto de las herramientas de QoS, es aquí que las políticas de negocio, las prioridades, y así sucesivamente empiezan a aplicarse.

Las inscripciones pueden entonces ser utilizadas por otras herramientas. Por ejemplo, los paquetes pueden ser desechados por las herramientas de políticas para que la velocidad de transferencia máximo en una interfaz no sea excedida. O los paquetes pueden ser desechados por las herramientas que evitan la congestión para evitar anticipadamente que se congestione la interfaz. El Resto de paquetes son entonces puestos en la cola, una vez más de acuerdo a sus marcas, y programados para la salida en la interfaz. Otras herramientas, tales como compresión, se pueden aplicar en la interfaz para reducir el ancho de banda consumido por el tráfico.

En las secciones siguientes se explora estas herramientas de QoS:

- Clasificación y marcación
- Políticas y modelado
- Evitar la congestión
- La gestión de la congestión
- Herramientas específicas de la capa de enlace

2.10.7.1. Clasificación y marcación

La clasificación es el proceso de análisis de paquetes y la clasificación en diferentes categorías a fin de que puedan ser debidamente marcados; después de que son marcados, los paquetes pueden ser tratados adecuadamente.

Marcar es el proceso de poner una indicación de la clasificación de los paquetes dentro del mismo paquete para que pueda ser utilizada por otras herramientas.

El marcado de la Capa 2 no son útiles como indicadores de QoS de extremo a extremo porque los medios de comunicación a menudo cambian a través de la red (por ejemplo, de Ethernet a un Frame Relay de área amplia red [WAN]). De este modo, el marcado en la Capa 3 es necesario para apoyar la QoS de extremo a extremo

- El Marcado en el campo ToS dentro de una cabecera de paquete IPv4, indica, el tipo de tráfico que se encuentra en el paquete. La presencia de esta marca puede ser utilizada por otras herramientas dentro de la red para proporcionar al paquete el servicio que necesita.
- Los primeros 6 bits en el campo de ToS se conoce como el DSCP bits.

2.10.7.2. Las clases de tráfico

- Clase de enrutamiento IP, Esta clase es para el tráfico del protocolo de enrutamiento IP, tales como Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), y así sucesivamente.
- Clase de Voz, Esta clase es para tráfico que porta Voz sobre IP (VoIP) (la conversación de tráfico), no para el tráfico asociado a la codificación, el cual iría en la clase de codificación de llamadas.
- Video Interactivo, Esta clase es para el tráfico de videoconferencia IP.
- Vídeo simultaneo, Esta clase es unicast o multicast de video unidireccional.
- Clase de datos de misión crítica, Esta clase está destinada a un subconjunto de los datos de aplicaciones transaccionales que son más importantes para la empresa. Las aplicaciones de esta clase son diferentes para cada organización.
- Clase de codificación de llamada, Esta clase está destinada para el tráfico de codificación de la voz y vídeo a la señalización.
- Clase de Datos transaccionales, Esta clase está destinada para las aplicaciones interactivas con el usuario tales como acceso a bases de datos, transacciones, y mensajería interactiva.
- Clase de Administración de red, Esta clase está destinada al tráfico de protocolos de gestión de la red, tales como SNMP.

- Clase de Volúmenes de datos, Esta clase está destinada al fondo, tráfico no interactivo, tales como transferencias de archivos de gran tamaño, distribución de contenido, sincronización de bases de datos, las operaciones de copia de seguridad, y correo electrónico.
- Clase de buscador de minas, Esta clase se basa en un proyecto de Internet 2 que define un servicio de "menos-que-mejor esfuerzo". Si se convierte en un enlace congestionado, esta clase, se eliminará de manera agresiva. Cualquier tráfico no relacionado al negocio (por ejemplo, la descarga de música en la mayoría de las organizaciones) se podría poner en esta clase.
- Clase de Mejor Esfuerzo, Esta clase es la clase por defecto. A menos que una aplicación haya sido asignada a otra clase. La mayoría de las empresas tienen cientos, si no miles, de aplicaciones a sus redes, la mayoría de estas aplicaciones siguen en la Clase de Mejor Esfuerzo.

Application	L3 Classification			L2 COS
	IPP	PHB	DSCP	
IP Routing	6	CS6	48	6
Voice	5	EF	46	5
Interactive Video	4	AF41	34	4
Streaming Video	4	CS4	32	4
Mission-Critical Data	3	AF31	26	3
Call Signaling	3	CS3	24	3
Transactional Data	2	AF21	18	2
Network Management	2	CS2	16	2
Bulk Data	1	AF11	10	1
Scavenger	1	CS1	8	1
Best Effort	0	0	0	0

Figura 18: Clasificación de tráfico para QoS

2.10.7.3. Políticas y Encolado

Herramientas de políticas desechan el exceso de tráfico o el modificar su marcado.

Herramientas de encolado almacenan en la memoria temporal los datos adicionales hasta que puedan ser enviados, por lo tanto, retrasa pero desecha.

2.10.7.4. Evitar la congestión

Técnicas para evitar la congestión supervisan las cargas de tráfico de la red a fin de que la congestión se pueda anticipar y así evitarla, antes de que sea problemático.

Si la Técnicas para evitar la congestión no se utilizan y una interfaz se llena, la cola por completo, los paquetes que traten de ingresar a la cola serán descartados, independientemente del tráfico que posean. Esto se conoce como cola para desechar, los paquetes que llegan al final de la cola serán descartados

Por el contrario, Si la Técnicas para evitar la congestión, permiten flujos de paquetes identificados como elegibles para descartar principios (éstos tienen prioridad más baja) que serán desechados cuando la cola esté llena.

Evitar la congestión funciona bien con tráfico basado en TCP basado; TCP incorpora un mecanismo de control de flujo de modo que cuando el origen detecta un paquete descartado, la fuente frena su transmisión.

Detección temprana aleatoria ponderada (WRED) de Cisco es la implementación del mecanismo de detección temprana al azar (RED). Paquetes descartados aleatoriamente RED cuando la cola llega a un determinado nivel (en otras palabras, cuando está casi lleno). RED está diseñado para trabajar con el tráfico TCP: Cuando los paquetes TCP son descartados, el mecanismo de control de flujo TCP disminuye la tasa de transmisión y entonces progresivamente comienza a aumentarla de nuevo. RED, por lo tanto, los resultados en las fuentes disminuyendo su flujo y ayudan a evitar la congestión.

WRED extiende RED utilizando precedencia IP en la cabecera del paquete IP para determinar que tráfico debe suprimirse; el proceso de selección y descartado se pondera por la precedencia IP. Del mismo modo, WRED basado en DSCP utiliza el valor DSCP en la cabecera del paquete IP en el proceso de selección y descartado. WRED selectivamente descarta tráfico

de menor prioridad (y de preferencia mayor o descartado por DSCP) cuando la interfaz comienza a congestionarse.

A partir de IOS Release 12.2 (8) T, Cisco ha puesto en marcha una ampliación de WRED llamado notificación explícita de congestión (ECN), que se define en el RFC 3168, la incorporación notificación explícita de congestión (ECN) para IP, y utiliza los 2 bits inferiores en el byte de ToS (como se muestra en la figura anterior 18). Dispositivos, utilizan éstos dos bits ECN para comunicar que están experimentando congestión. Cuando ECN está en uso, este marca los paquetes como que experimentan congestión (en lugar de desecharlos) en caso de los remitentes tengan capacidades de ECN y la cola aún no ha llegado a su límite máximo. Si la cola no llega al máximo, los paquetes son descartados al no tener ECN.

2.10.7.5. La gestión de la congestión

Como el nombre implica, los controles de gestión de la congestión después de que la congestión se ha producido. Por lo tanto, si no existe congestión, estas herramientas no son provocadas, y los paquetes se envían a cabo tan pronto como llegue a la interfaz.

La gestión de la congestión pueden ser considerada como dos procesos separados: encolado, que separan el tráfico en varias colas o buffers, y la programación, que decide cual tráfico de cola se enviará a continuación.

2.10.7.6. Herramientas específicas de la capa de enlace

Herramientas específicas del enlace son las que están habilitadas en ambos extremos de un punto a punto conexión WAN para reducir el ancho de banda requerido o el retraso experimentado en ese enlace. Las herramientas QoS disponibles incluyen la compresión de cabecera (para reducir la utilización del ancho de banda) y enlazar la fragmentación y entrelazados (LFI) (para reducir el retraso encontrado).

CAPÍTULO III

3. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED INFORMÁTICA DEL H. CONSEJO PROVINCIAL DE TUNGURAHUA

3.1. Antecedentes de la Red Informática

La red informática fue implementada en octubre del año 2002 con cableado estructurado categoría 5, se poseía 79 computadores, se encontraban interconectadas las direcciones del edificio matriz, se utilizaba el servicio de internet dial-up; durante los años siguientes se han incorporado equipos para la administración de Internet, correo electrónico corporativo, servidores de bases de datos, servidor de dominio y DNS para administrar los usuarios y recursos de red, servidor de respaldo de datos para las bases de datos, y se ha incorporado enlaces espectro ensanchado para interconectar otras dependencias remotas, además de integrar los departamentos con la tecnología inalámbrica.

Para el año 2008 se ha incrementado a 165 dispositivos de red entre computadores, servidores, equipos inalámbricos, enlaces espectro ensanchado, relojes biométricos y puntos de impresión en red,

interconectado el edificio matriz y las dependencias de Bodega, Talleres y el Centro de Promociones y Servicios de la Provincia, con los principales servicios de red como: internet corporativo (proxy), correo corporativo, automatización de procesos de solicitud de compras, seguridad de navegación, dominio de red, recursos compartidos y usuarios así como también la utilización de antivirus corporativo.

Detalle del desarrollo tecnológico del HCPT

Año	Dispositivos de red	Principales Acciones Realizadas	Principales Servicios
2002	79	- Conexiones entre cada dirección sin fundamentar políticas, grupos de trabajo ni seguridad.	-Internet
2003	101	- Configuración del servidor de correo interno sobre Solaris. - Se establece grupos de trabajo y direcciones locales para conexión - Se realiza el proyecto del préstamo del BEDE para la compra del servidor Lotus, Oracle, y 2 conmutadores para el incremento de nuevos equipos - Registro de Dominio y Hosting para el sitio tungurahua.gov.ec	-Correo interno
2004	110	- Se instala el Servidor Lotus y Oracle para el desarrollo de Base de Datos como principal procesos de automatización se realiza las Solicitudes de Compra y PFs - Configuración del Servidor de Internet para control de sitios restringidos - Rediseño del sitio web tungurahua.gov.ec	-Correo Corporativo -Aplicaciones Lotus - Servidor Proxy
2005	122	- Interconexión de las dependencias de Talleres, Centro Promociones y Servicios - Servidor de dominio para la administración y control de recursos de red, y DNS para el acceso al Sitio Web	-Difusión de la red -DNS Interno
2006	146	- Se crea el dominio interno para la red hcpt.gov.ec - Firewall para protección de Internet a nivel de datos, - Relojes Biométricos para el control de personal - Se desarrolla sistemas de Administración y Control de Personal y Médico Odontológico - Se incrementa más equipos para lo cual se establece puntos de acceso inalámbricos en cada dirección - Se actualiza el sitio web conforme la Ley de Transparencia	-Dominio de red -Seguridad Firewall -Interconexión Inalámbrica -Portal Web

Año	Dispositivos de red	Principales Acciones Realizadas	Principales Servicios
2007	150	- Se instala un servidor de prueba para el control de antivirus - Servidor de Respaldos Lotus y Oracle - Se incrementa las funcionalidades del sistema de personal. - Seguridad en el Control en Acceso inalámbrico I Etapa	-Antivirus corporativo - Seguridad Wireless
2008	165	▪ Se adquiere un equipo de red CISCO dedicado exclusivamente para el núcleo de la red ▪ Se plantea hacer un rediseño completo de la tecnología y topología de red, para incrementar las seguridades, y velocidad de navegación	-Redes locales Virtuales - Segmentos de red -Incremento del ancho de banda

Tabla 2: Evolución tecnológica del HCPT

No existe una Dirección o Departamento de Tecnologías de la Información y Comunicación, que se encargue de realizar, ejecutar y evaluar una planificación informática de la institución.

Existe únicamente una Área de Informática, con dos profesionales de sistemas, que se encargan de cumplir con las actividades de informática de toda la institución como: planificación informática de la unidad, administración de internet, redes y correo electrónico, administración de sistemas y bases de datos, mantenimiento de equipos y asesoramiento a todo el personal.

A continuación se detalla el Estructura orgánica funcional del HCPT

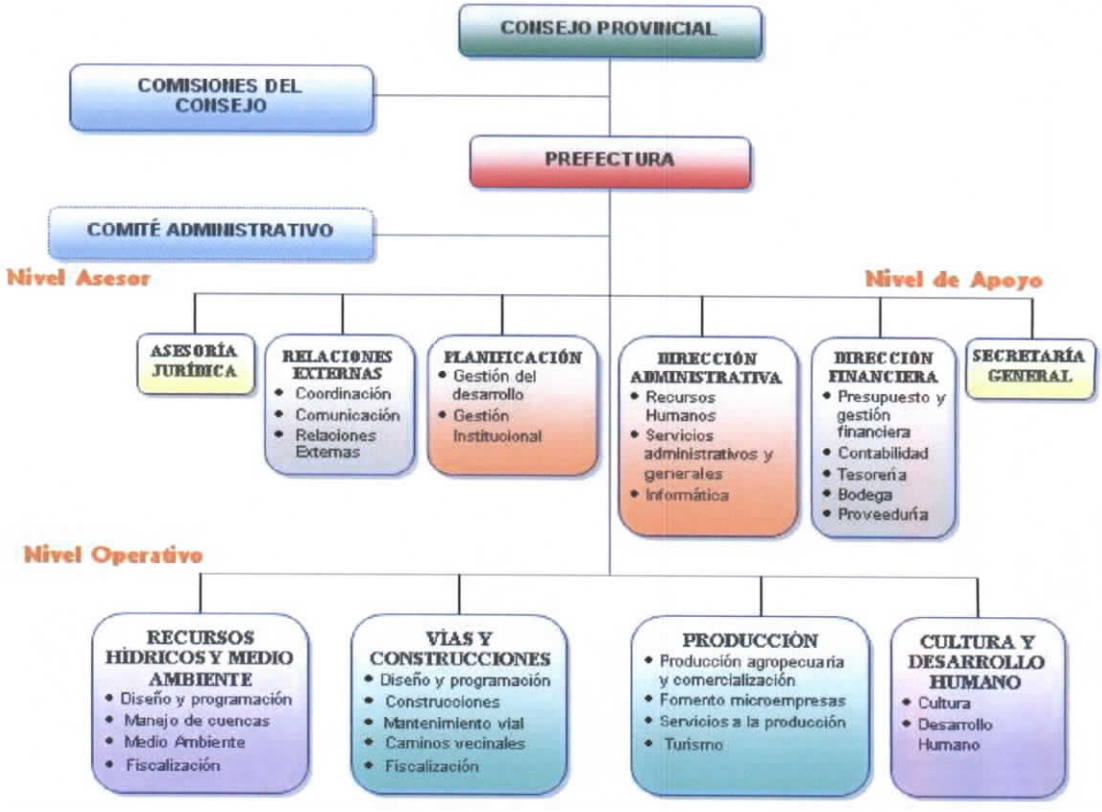


Figura 19: Organigrama del HCPT

Por lo que se puede apreciar en la Figura 19, la unidad de Informática forma parte de la Dirección Administrativa, y es concebida como una unidad de apoyo.

Se debería primeramente reorganizar esta Unidad para convertirla al nivel Asesor, como Departamento de Tecnología de la Información y Comunicación o Telemática y, que de esta manera permita ayudar en la toma de decisiones de la institución, y encargarse de la gestión de proyectos de tecnología institucionales

3.2. Inventario de los recursos tecnológicos de la red

El inventario de los equipos y dispositivos de red existentes se detalla a continuación, los cuales se determinaron utilizando herramientas libres, que permiten adquirir la información requerida como tipo de recurso, nombre de recurso (hostname y NETBIOS), grupo o dominio al cual pertenece, dirección IP, dirección física (MAC Address), velocidad de conexión, puertos abiertos, SSID, etc. Clasificándola de acuerdo al departamento al cual pertenece.

De lo cual tenemos que existen 165 dispositivos entre Servidores, Computadores, Access points, Firewwall, Modem ADSL, Impresoras, equipos de seguridad y equipos biométricos que conforman la red.

En el Anexo 1 se muestra el inventario de los equipos de red.

3.3. Clasificación de dispositivos de red

La siguiente etapa de este proyecto es la clasificación de los dispositivos recopilados, por lo cual tenemos lo siguiente tipos Modem ADSL, Firewall, Switchs, Routers, Access Points, Servidores, Computadores, Impresoras y Otros dispositivos, en el siguiente cuadro se presenta un listado de los dispositivos principales tales como Computadoras, servidores, Impresoras y Access Points por dirección o dependencia.

Computadores, Servidores, Impresoras y Access Points de red

No	Dirección	PCs	Serves	Impresoras		Access Point
1	Desarrollo Humano y Cultura	6		4	4 l	1
2	Secretaría General	6		8	3 l, 4 i, 1 m	1
3	Relaciones Externas	4		3	1 l, 2 i	1
4	Sala de Choferes	1				
5	Financiero	16	1	14	5 l, 4 i, 5 m	2
6	Recursos Hídricos	17		10	1 p, 2l, 7 i	1
7	Sala de Consejeros	2		1	1 i	
8	Vías y Construcciones	13		10	1p, 1, 8 i	
9	Procuraduría Síndica	4		2	1 l, 1 i	1
10	Planificación	6		7	1 p, 1 l, 5 i	1
11	Producción	12		6	6 i	1
12	Administrativo	13		6	1 l, 4 i, 1 m	1
13	Sistemas	4	4	1	1 i	
14	Cooperativa	1		1		
15	Talleres	1		1	1 i	
16	Bodega	3		3	2 i, 1 m	1
17	Gobierno Provincial	17	1	2	1 l, 1 i	1
18	Aula Virtual	1				
	Totales	**129**	**6**	**76**		**12**

Tabla 3: Dispositivos de red por direcciones

Luego se debe indicar los servidores del HCPT y sus aplicaciones, que están en el rack principal de comunicaciones ubicado en el cuarto de servidores

Detalle de servidores

No.	Nombre	Descripción	Sistema Operativo	Aplicaciones
1	Sunfirev120	Servidor Proxy de internet	Solaris 9	Squid-cache
2	SunFire280r	Servidor de Correo Electrónico Interno	Solaris 9	Lotus Domino
3	SunFireV440	Servidor de Bases de Datos	Solaris 10	Oracle 10g
4	ServerHCPT	Servidor de Dominio, DNS y Antivirus	Windows 2003 Server Enterprise	Active Directory Symantec EndPoint Protection 11

No.	Nombre	Descripción	Sistema Operativo	Aplicaciones
5	ServidorDF	Servidor de Sistema Contable FINANSG	Windows 2000 Advanced Server	SQL Server 2000 FINANSG
6	ServidorHP	Servidor de Aplicación Mapeo de Actores	Linux Fedora 10	Sistema de Mapeo de Actores MySQL

Tabla 4: Detalle de Servidores

A continuación se indican los dispositivos de conmutación Switchs de los que se dispone y que están dentro del rack principal de Sistemas, son administrables, vía web y consola vía puerto serial RS-232.

Detalle de Switchs

Cant	Marca y Modelo	Características Generales
2	3COM SuperStack 3 Switch 4226T - 3C17300 Switch Capa 2	24xEthernet 10Base-T, Ethernet 100Base-TX 2x10/100/1000Base-T SNMP, RMON IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p Control de flujo, capacidad duplex, auto-sensor por dispositivo, negociación automática, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), activable, apilable RS-232 Serial port.
2	3COM SuperStack 3 Switch 3300XM - 3C16985B Switch Capa 2	24xEthernet 10Base-T, Ethernet 100Base-TX 1xStacking Connector SNMP, RMON IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p Control de flujo, capacidad duplex, auto-sensor por dispositivo, negociación automática, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), activable, apilable. RS-232 Serial port
1	Cisco Catalyst 3560G-48PS Witch Capa 3	48 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T 4 x SFP (mini-GBIC) IEEE 802.3ab, IEEE 802.3af Alimentación por Ethernet (PoE) Soporta Ruteo VLANS

Tabla 5: Detalle de Switchs

Otro dispositivo de red que también posee el HCPT, es el Firewall de la red, que también está dentro del rack principal de sistemas y es administrable vía web, posee sistema operativo basado en Linux.

Detalle del firewall

Cant	Marca y Modelo	Características Generales
1	Symantec Gateway Security 1600 Series	DoS Prevention • Intrusion Prevention • Blacklist Spam Filtering • Content Filtering • Network Antivirus IPSec • PPPoE • PPTP OSPF • RIP Version 2 DHCP Server • Relay HTTP • SSL Remote Management Protocol RADIUS • RSA SecurID • LDAP • POP3 Actualmente este equipo no tiene actualizada las licencias de: subscripción de antivirus y antispam, subscripción de la Base de datos del filtrado de contenido y la subscripción de la base de datos de detección y prevención de intrusiones. Y este equipo ya no tiene soporte por parte del fabricante.

Tabla 6: Detalle del Firewall

Para la conexión a internet como ya se mencionó anteriormente, se tiene contratado un servicio ADSL de 1024 kbps de subida y 512 kbps de bajada con la empresa Andinanet, este dispositivo se encuentra en calidad de préstamo hasta culminar el contrato, y también se encuentra en el rack principal de comunicaciones.

Detalle del modem ADSL de conexión a internet

Cant	Marca y Modelo	Características Generales
1	Huawei SMARTAX MT 800	ITU G.992.1 (G.dmt) Annex A, ITU G.992.2(G.lite), ITU G.994.1(G.hs), ANSI T1.413 Issue # 2 1 puerto WAN RJ-11 ADSL 1 Puerto LAN 10/100 Base T Ethernet DHCP server, NAT/NAPT , PAP/CHAP, IP Filter, Firewall, bloqueo de protocolo

Tabla 7: Detalle del Modem ADSL

Esquema del Rack principal de dispositivos de conexión a red y de servidores

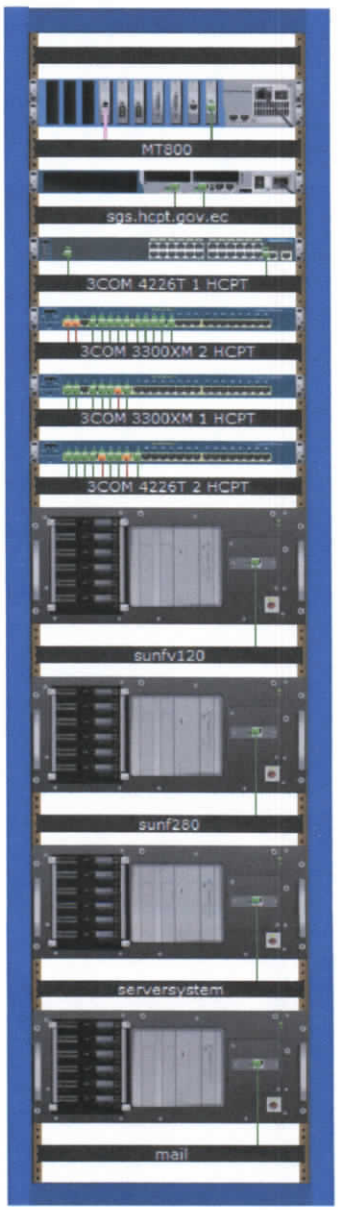


Figura 20: Esquema del Rack Principal de red

A continuación se muestra una vista real del rack principal del cuarto de servidores.

Figura 21: Rack principal de servidores del HCPT

Para el servicio de red inalámbrica se tienen los siguientes dispositivos de comunicación, a través de todas las infraestructuras físicas del HCPT, que funcionan como puntos de acceso y bridge, ver Anexo 3, Anexo 4, Anexo 5 y Anexo 6.

Detalle de Puntos de Acceso

Cant	Marca y Modelo	Características Generales
10	Proxim ORiNOCO® AP-4000	IEEE 802.11a 5GHz, OFDM IEEE 802.11b/g 2.4 GHz DSSS, OFDM CSMA/CA 15 FFC Canales Seguridad 802.1X and TKIP, WPA, AES and 802.11i DHCP, Telnet, HTTP, TFTP, Boot P, and SNMPv2C 802.11i-D3 Antena omni 3dBi Authentication 802.1X RADIUS-based MAC address RS-232 Serial port
4	TEW-430APB 802.11g Wireless Access Point	Access point, Bridge, Repetidores Wireless 64/128 bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK 802.1x, Filtrado de MAC 20 entradas Habiltar/Desbilitar broadcast ESSID Puerto FastEthernet 10/100 Mbps auto sensitivo Tasa transferencia 54,48,36,21,18,12,9,y 6 Mbps en 802.11g Tasa transferencia 11,5.5,2,y 1 Mbps en 802.11b Antena interna de 2 dBi Configuración vía Web Browser HTTP
3	Senao Wireless Solution Provider NCB-8610	802.11b Access point, Bridge, Repetidores Wireless 64/128 bit WEP, WPA/WPA2 802.1x, Filtrado de MAC 32 entradas 14 canales
2	Linksys WAP54G	IEEE 802.11b, IEEE 802.11g TCP/IP, IPX/SPX, NetBEUI/NetBIOS IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11g WEP de 128 bits, encriptación de 64 bits WEP, WPA de 256 bits 1x Ethernet 100Base-TX

Tabla 8: Detalle de Access Points

A continuación se muestra un detalle de los servicios que están disponibles en equipos de comunicación inalámbricos, ubicación, estándares, tipo de clave de seguridad, filtrado por direcciones físicas, nombre de SSID, etc.

Detalle de servicios de los puntos de acceso inalámbricos por direcciones

Dirección	Nombre	Ubicación	Estándar	SSID	WEP	DHCP	MAC	PC
Administrativo	ORiNOCO-AP-4000 -5b-6f-52	6to Piso Edificio Central	802.11g	HCPT_ADM _G1	NO	SI	SI	13
Bodega y Talleres	TEW-430APB 802.11g Wireless Access Point	Terraza Edificio Central	802.11g	Extreme2	SI	NO	SI	
Bodega y Talleres	TEW-430APB 802.11g Wireless Access Point	Terraza Sindicato HCPT	802.11g	Extreme2	SI	NO	SI	
Bodega y Talleres	AP_BOD_B1	Terraza Sindicato HCPT	802.11b	AP_BOD_B1	SI	NO	SI	
Bodega y Talleres	AP_BOD_B2	Terraza Talleres	802.11b	AP_BOD_B1	SI	NO	SI	1
Bodega y Talleres	AP_BOD_B3	Terraza Bodega	802.11b	AP_BOD_B1	SI	NO	SI	
Bodega	ORiNOCO-AP-4000-5b-98-1c	Oficina de Bodega	802.11g	HCPT_BOD _G1	SI	NO	SI	3
Cultura	ORiNOCO-AP-4000-5b-25-ce	Planta Baja Edificio Central	802.11g	HCPT_DHC _G1	SI	NO	SI	6
Financiero	ORiNOCO-AP-4000-59-c7-0f	2do Piso Edificio Central	802.11g	HCPT_FIN_ G1	SI	NO	SI	8
Financiero	Linksys WAP54G	2do Piso Edificio Central	802.11g	HCPT_FIN_ G2	SI	NO	SI	7
Gobierno	TEW-430APB 802.11g Wireless Access Point	Terraza Edificio Central	802.11g	Extreme1	SI	NO	SI	1
Gobierno	TEW-430APB 802.11g Wireless Access Point	Terraza Centro Promociones y Servicios	802.11g	Extreme1	SI	NO	SI	
Planificación	ORiNOCO-AP-4000-5b-69-5c	5to Piso Edificio Central	802.11g	HCPT_PLA N_G1	SI	SI	SI	10
Producción	ORiNOCO-AP-4000-62-52-db	5to Piso Edificio Central	802.11g	HCPT_PRO _G1	SI	NO	SI	10
Recursos Hídricos	ORiNOCO-AP-4000-5b-25-dd	3er Piso Edificio Central	802.11g	HCPT_RRH H_G1	SI	NO	SI	16
Relaciones Externas	ORiNOCO-AP-4000-5d-68-a0	1er Piso Edificio Central	802.11g	HCPT_REX _G1	NO	SI	SI	2
Sala de Consejeros	Linksys WAP54G	Tercer Piso Edificio Central	802.11g	HCPT_CON _G1	SI	NO	SI	1
Secretaria	ORiNOCO-AP-4000-5d-68-c4	Primer Piso Edificio Central	802.11g	HCPT_SEC _G1	SI	NO	SI	6
Vías y Construcciones	ORiNOCO-AP-4000M-70-7b-c5	Cuarto Piso Edificio Central	802.11g	HCPT_OOP P_G1	SI	NO	SI	12

Tabla 9: Características de los Access Points

Existen 5 puntos de red para impresión, ubicados en los departamentos que tienen mayor carga de documentación, como es la Dirección, Administrativa, 4 de ellos son impresoras Laser de marca Xerox Workcenter M123 que permiten las funciones de copia, fax, impresora, como se indica en la figura 22.

Figura 22: Puntos de impresión en red

Y la otra impresora que está conectada a la red es un plotter HP deskjet 550 para la impresión de planos y se encuentra ubicada en la área de planos de la Dirección de Recursos Hídricos, como se indica en la figura 4.

Figura 23: Plotter HP en red para la impresión de planos

También están los equipos de control biométrico que se utilizan para el registro de la asistencia, y el control de las horas, de trabajo, éste se encuentra conectado a la red para descargar sus datos en el Sistema de Control de Recursos Humanos, existen 2 unidades, ubicados en el hall de la planta baja del HCPT y en la oficina de Recursos humanos de Talleres del HCPT.

Reloj Biométrico HP-2000 del Hall de la Planta Baja del HCPT

Figura 24: Reloj Biométrico del HCPT

Por último está el equipo de seguridad cuyo monitor central se encuentra conectado a la red y permite monitorear desde cualquier computador las cámaras de seguridad.

Monitor del Equipo de Seguridad

Figura 25: Monitor de las Camaras de Seguridad

3.3.1. Licenciamiento de computadores

Los sistemas operativos de las estaciones de trabajo es Microsoft Windows en sus versiones: Windows Vista, XP, 2000 Advanced Server, Millennium y 98

De las cuales el 81% de los equipos utilizan Windows XP, quedando el 9% que utiliza una versión anterior del sistema Windows, y del total de los equipos sólo el 48% posee licenciamiento de uso del sistema operativo.

Figura 26: Sistema operativo de las estaciones de trabajo

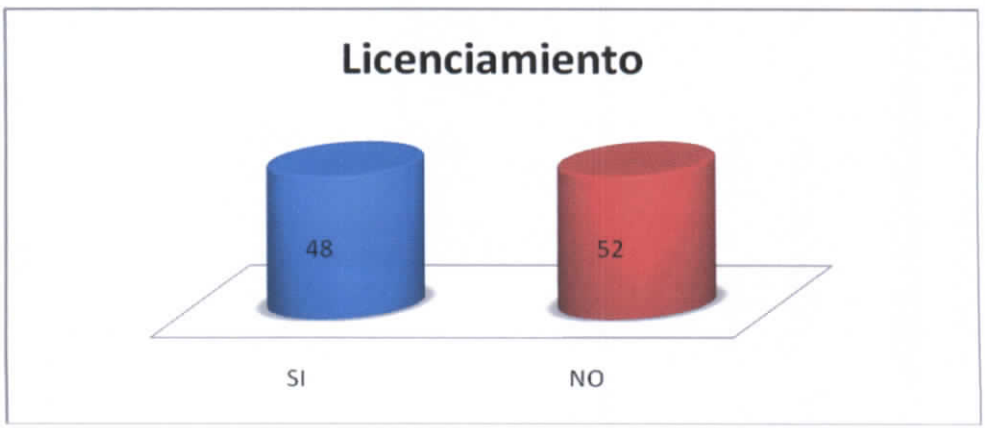


Figura 27: Porcentaje de sistema operativo licenciado

Por lo que se tendría que actualizar el sistema operativo en un 90% para migrar a la nueva tecnología existente de Windows Vista, e incluir una alternativa de licenciamiento corporativo con servicio de aseguramiento de renovación, o buscar alternativas con software libre, pero algunas aplicaciones como manejo de planos y sistemas geográficos que se utilizan son realizadas en sistemas que corren bajo Windows.

3.4. Estructura de la red actual

El H. Consejo Provincial de Tungurahua posee las siguientes infraestructuras físicas, las cuales están interconectadas actualmente en red mediante enlaces Spread Spectrum de 2.4GHz, los cuales se encuentran legalmente registrados en la Secretaría Nacional de Telecomunicaciones, con su debido permiso de funcionamiento.

Estas infraestructuras son:

- Edificio Central del H. Consejo Provincial de Tungurahua
- Edificio Centro de Promociones y Servicios de la Provincia
- Bodega y Talleres

Estas Infraestructuras físicas por las distancias que tienen desde 120 metros a 2.6 kilómetros se pueden considerar que conforman una red de área metropolitana MAN ver Anexo 2.

Aquí se detalla un cuadro con las Coordenadas geográficas de todas las infraestructuras físicas del H Consejo Provincial de Tungurahua, y se indica si poseen conexión remota.

Ubicación	Área	Conexión 2.4 GHz	Coordenada X (Este)	Coordenada Y (Sur)	Altura (metros)
Edificio Central		SI	763726	9862589	2623
Gobierno Provincial		SI	763845	9862518	2604
Bodega Talleres		SI	764987	9863628	2570
Parque de la Familia	Administración	NO	760703	9862084	3019
	Información	NO	760619	9862149	3030
	Caseta Control	NO	760531	9862131	3028
Granja de Píllaro		NO	771574	9869914	2761
Vivero Catiglata		NO	766353	9863125	2501

Tabla 10: Coordenadas Geográficas de las dependencias del HCPT

A continuación se muestra una vista esquemática de interconexión remota

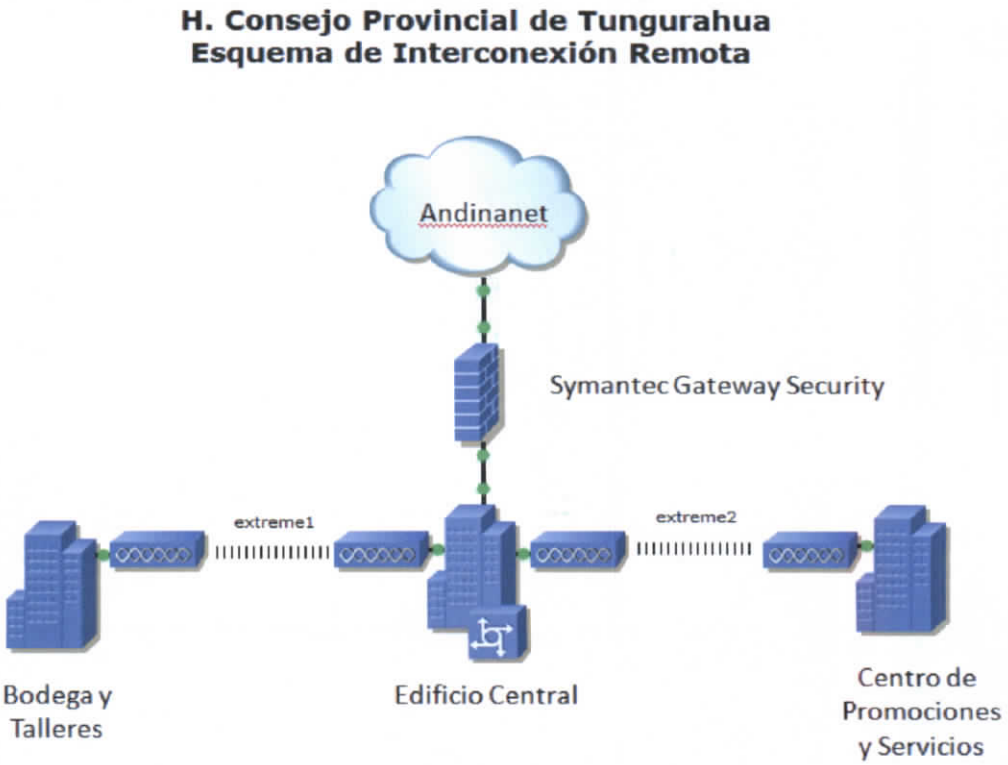


Figura 28: Esquema de Interconexión de Dependencias del HCPT

El servicio de conexión a Internet se tiene contratado con la empresa Andinanet el cual es un servicio ADSL con un ancho de banda actual de 1024Kbps de bajada y 512kbps de subida, utilizando un modem ADSL MT800 Huawei proporcionado por el proveedor con una dirección IP pública de 200.107.35.65 con máscara de red 255.255.255.248, es decir, se posee un rango de 6 IPs públicas 200.107.35.64/29

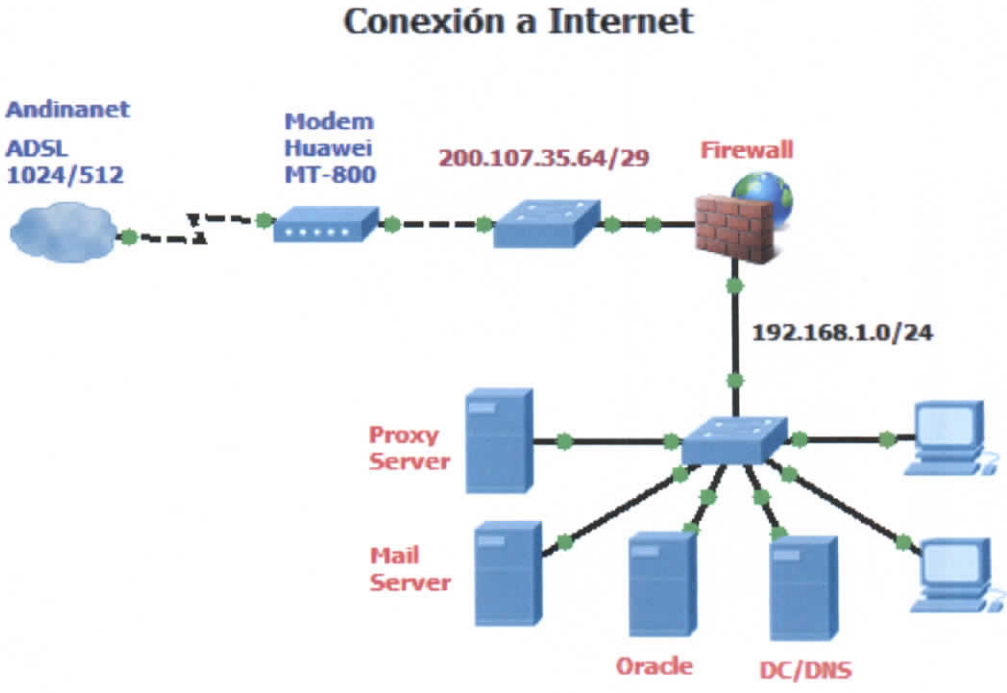


Figura 29: Esquema de la Conexión a Internet

La red interna tiene una dirección de red 192.168.1.0 con máscara de red 255.255.255.0 lo que se denomina una red plana, esto ocasiona que los paquetes informáticos que se generan sean difundidos a todos los

dispositivos de la red, aumentando el tráfico de peticiones y congestionando los servicios que poseen.

Continuando con la estructura de la red hay que mencionar cada dirección, departamento y área que posee el HCPT, por lo que a continuación se presenta un listado de sus dependencias y ubicación.

Detalle de dependencias del HCPT

Infraestructura	Dirección/Departamento/Área	Ubicación	Dirección
Edificio central	Cultura	Planta baja	Bolívar 491 y Castillo
	Secretaría General	Primer piso	
	Relaciones Externas	Primer piso	
	Financiero	Segundo piso	
	Recursos Hídricos	Tercer piso	
	Sala de Consejeros	Tercer piso	
	Vías y Construcciones	Cuarto piso	
	Planificación	Quinto piso	
	Procuraduría Síndica	Quinto piso	
	Producción	Quinto piso	
	Administrativo	Sexto piso	
	Sistemas	Sexto piso	
	Asociación Empleados	Séptimo piso	
	Cooperativa	Terraza	
	Antenas Spread Spectrum	Terraza	
Centro de promociones y servicios de la provincia	Aula Virtual	Planta baja	Sucre y Castillo
	Biblioteca Municipio Ambato	Mezzanine 1	
	Biblioteca H.C.P.T.	Mezzanine 2	
	Gobierno Provincial	Primer piso	
	Antenas Spread Spectrum	Primer piso	
Bodega y Talleres	Oficina de Talleres	Talleres	Av. González Suarez y Av. Las Américas
	Oficina de Bodega	Bodega	
	Antenas Spread Spectrum	Terraza Sindicato HCPT	

Tabla 11: Ubicación de las dependencias del HCPT

A continuación se muestran los planos de cada una de las dependencias físicas indicadas, el diagrama de conexión vertical, y horizontal, con un resumen de los dispositivos de red y de conexión que posee cada departamento.

Edificio Central del H. Consejo Provincial de Tungurahua, ubicado en las calles Simón Bolívar 491 y Mariano Castillo

Figura 30: Edificio Central de HCPT

Cableado vertical

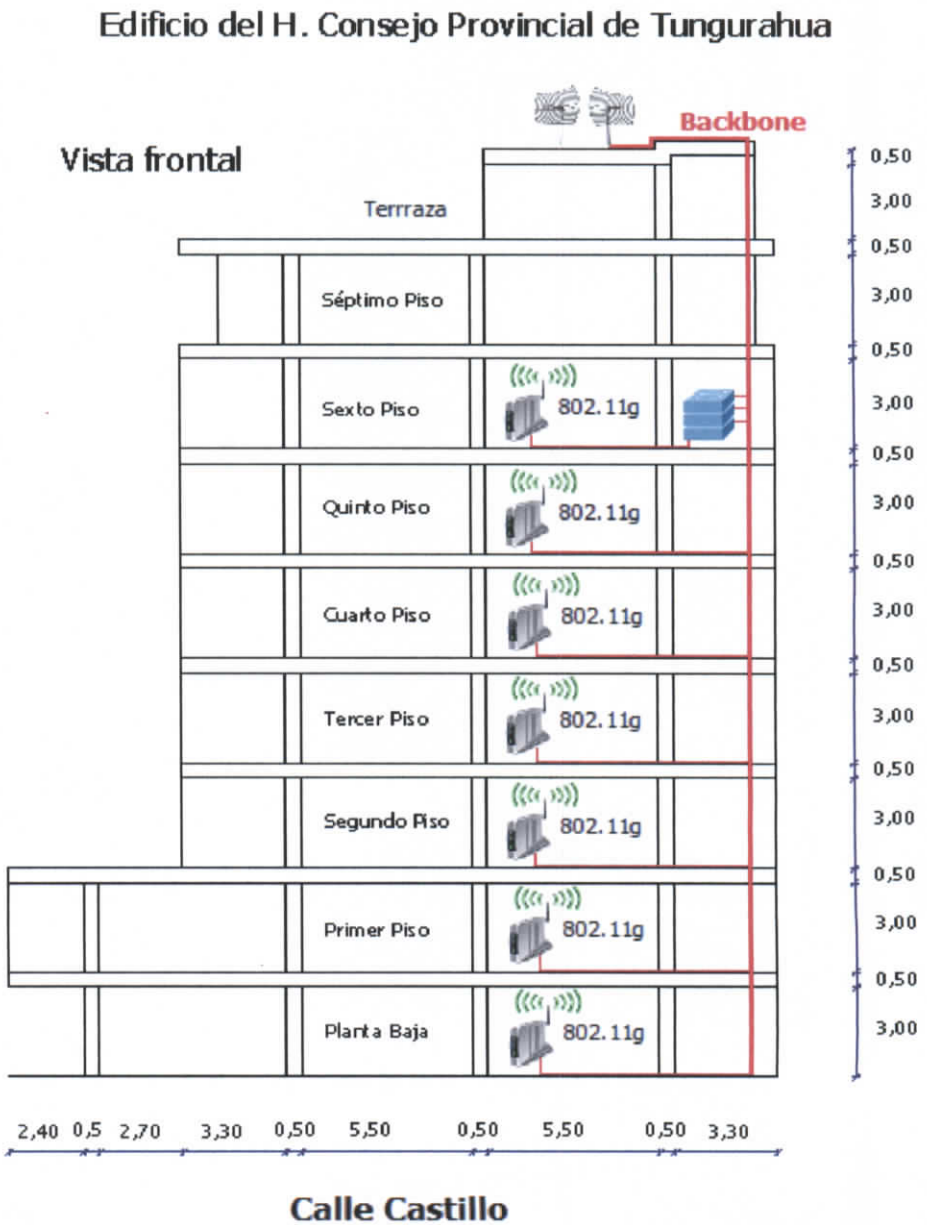


Figura 31: Vista lateral del Edificio Central desde la calle Castillo

Cableado Horizontal

Planta Baja: Desarrollo Humano y Cultura, y Recaudación

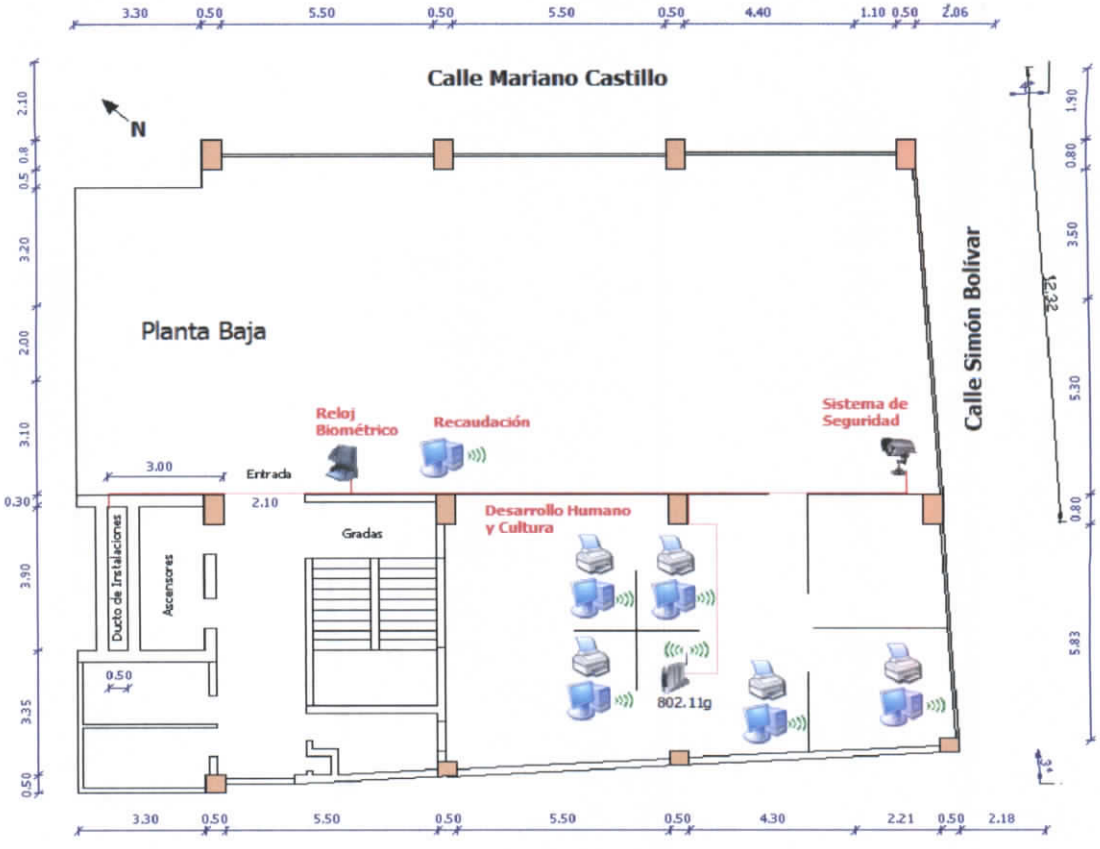


Figura 32: Vista de la planta baja del HCPT

Equipos	Conexión	SSID
1 Access Point	54 Mbps, 2.4GHz	HCPT_DHC_G1
6 PC	802.11g 54Mbps	6 HCPT_DHC_G1
1 Reloj Biométrico	Ethernet 10 Mbps	
1 Sistema de Seguridad	FastEthernet 100 Mbps	
Total 9 IPs		

Tabla 12: Resumen de Dispositivos de red de la planta baja

Primer Piso: Prefectura, Secretaría General y Relaciones Externas.

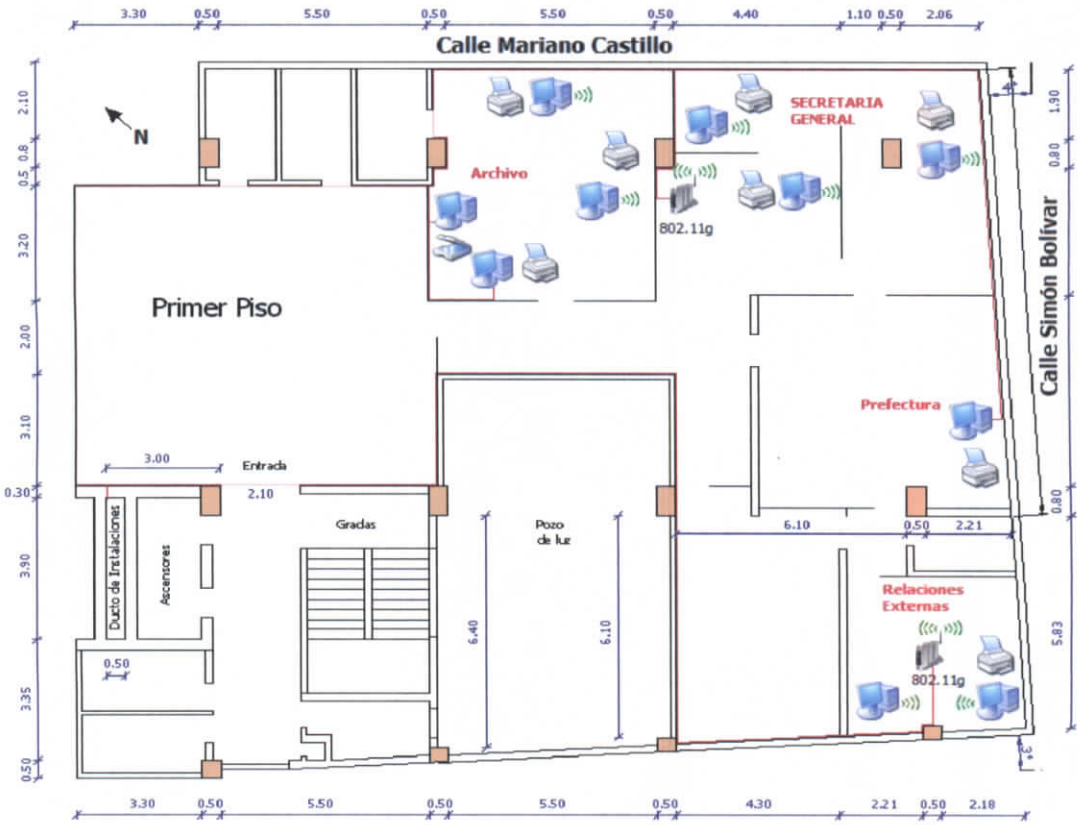


Figura 33: Vista del Primer piso del HCPT

Equipos	Conexión	SSID
2 Access Point	54 Mbps, 2.4GHz	HCPT_SEC_G1 HCPT_REX_G1
7 PC	802.11g 54Mbps	5 HCPT_SEC_G1 2 HCPT_REX_G1
3 PC	FastEthernet 100 Mbps	
Total 12 IPs		

Tabla 13: Resumen de dispositivos de red del primer piso

Segundo Piso: Dirección Financiera

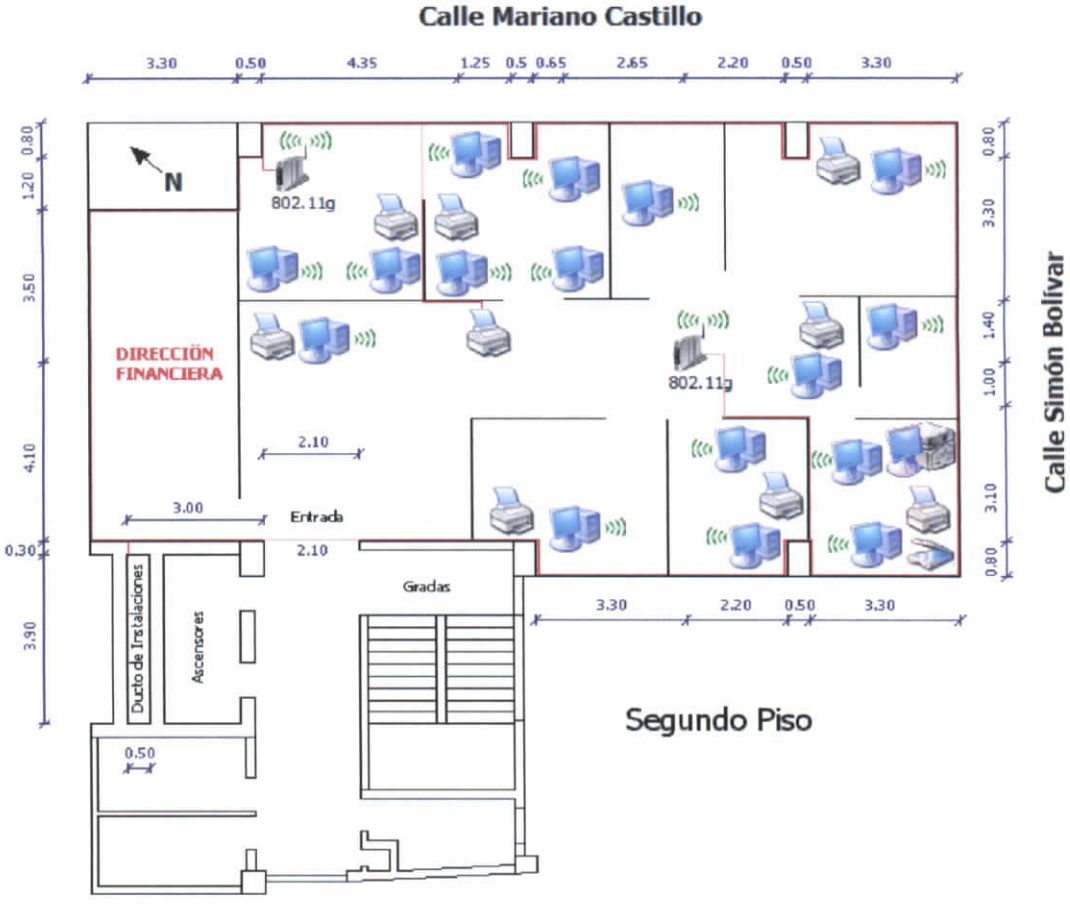


Figura 34: Vista del segundo piso del HCPT

Equipos	Conexión	SSID
2 Access Point	54 Mbps, 2.4GHz	HCPT_FIN_G1 HCPT_FIN_G2
16 PC	802.11g 54Mbps	8 HCPT_FIN_G1 7 HCPT_FIN_G2
1 Servidor HP Prolaint	FastEthernet 1000 Mbps	
1 Impresora Copiadora	FastEthernet 1000 Mbps	
Total 20 IPs		

Tabla 14: Resumen de dispositivos de red del segundo piso

Tercer Piso: Dirección de Recursos Hídricos

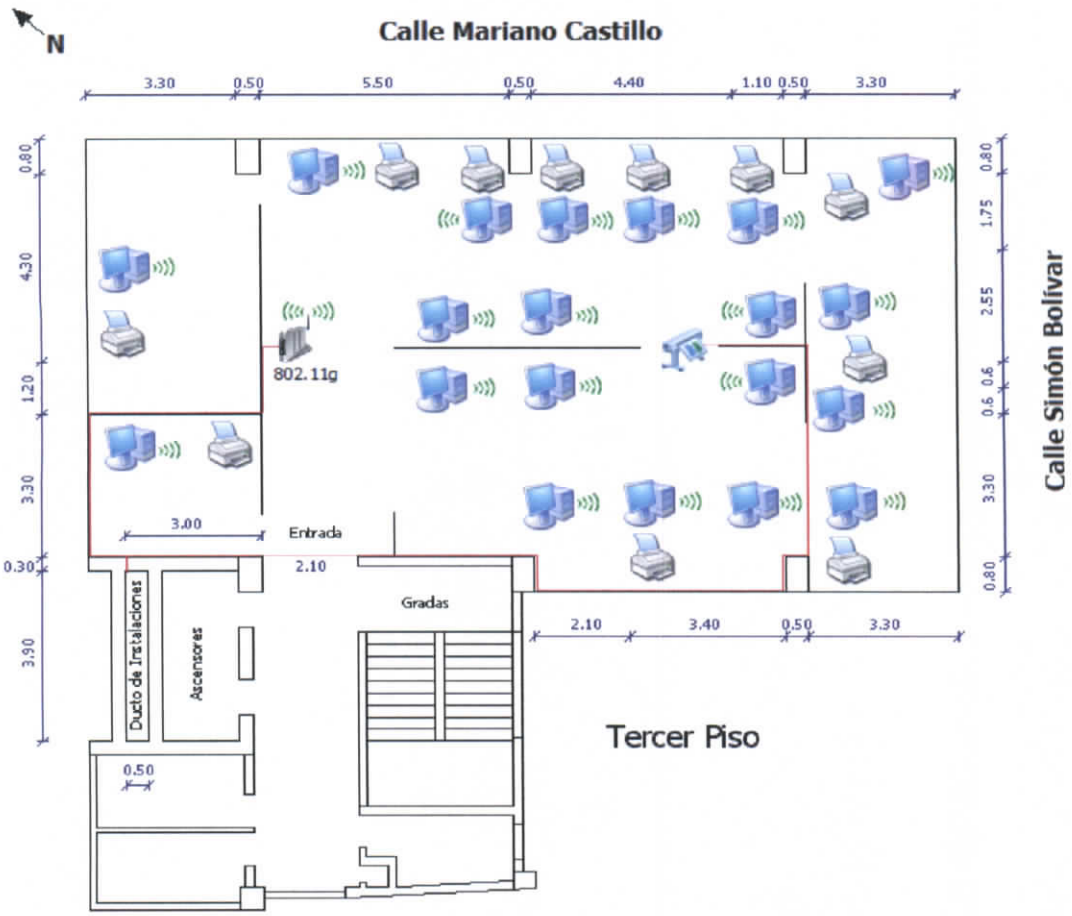


Figura 35: Vista del tercer piso del HCPT

Equipos	Conexión	SSID
1 Access Point	54 Mbps, 2.4GHz	HCPT_RRHH_G1
16 PC	802.11g 54Mbps	16 HCPT_RRHH_G1
1 Plotter HP 500 DeskJet	FastEthernet 100 Mbps	
Total 18 IPs		

Tabla 15: Resumen de dispositivos de red del tercer piso

Cuarto Piso: Dirección de Vías y Construcciones

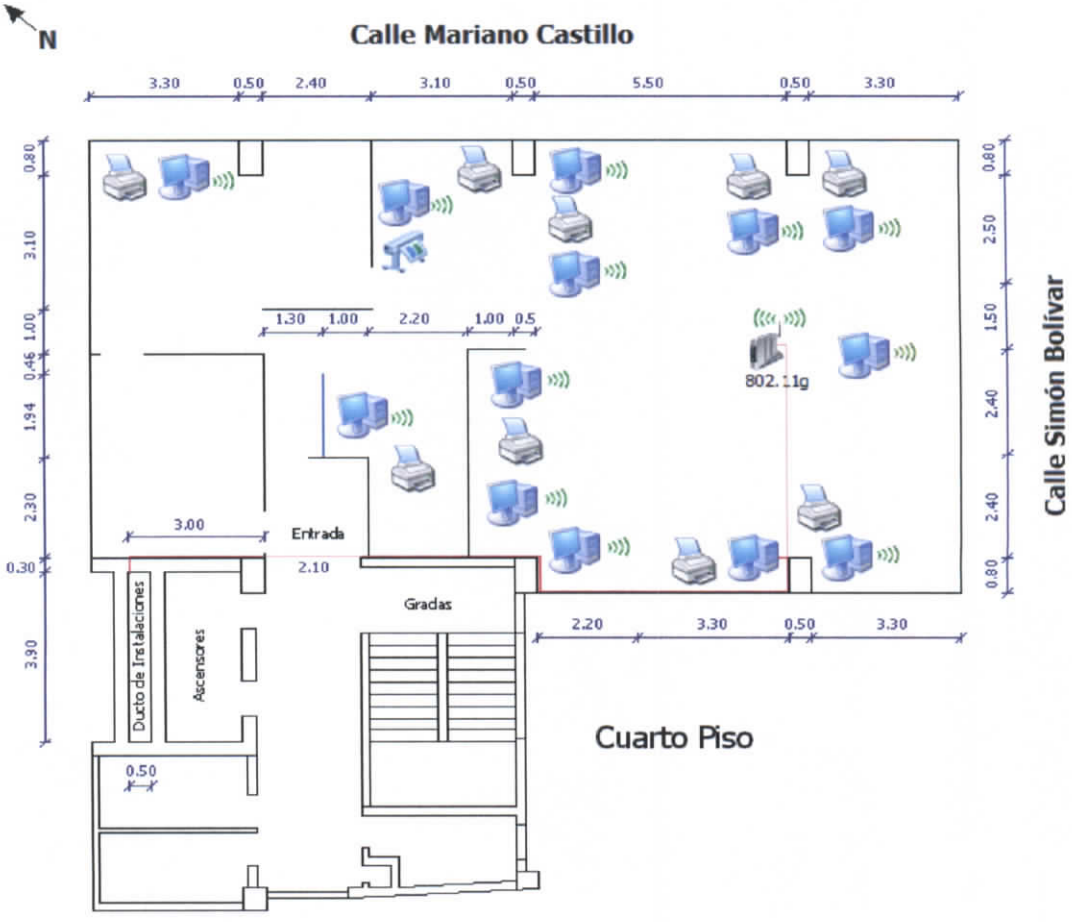


Figura 36: Vista del cuarto piso

Equipos	Conexión	SSID
1 Access Point	54 Mbps, 2.4GHz	HCPT_OOPP_G1
12 PC	802.11g 54Mbps	12 HCPT_OOPP_G1
1 PC	FastEthernet 100 Mbps	
Total 14 IPs		

Tabla 16: Resumen de dispositivos de red del cuarto piso

Quinto Piso: Direcciones de Planificación, Procuraduría Síndica y Producción

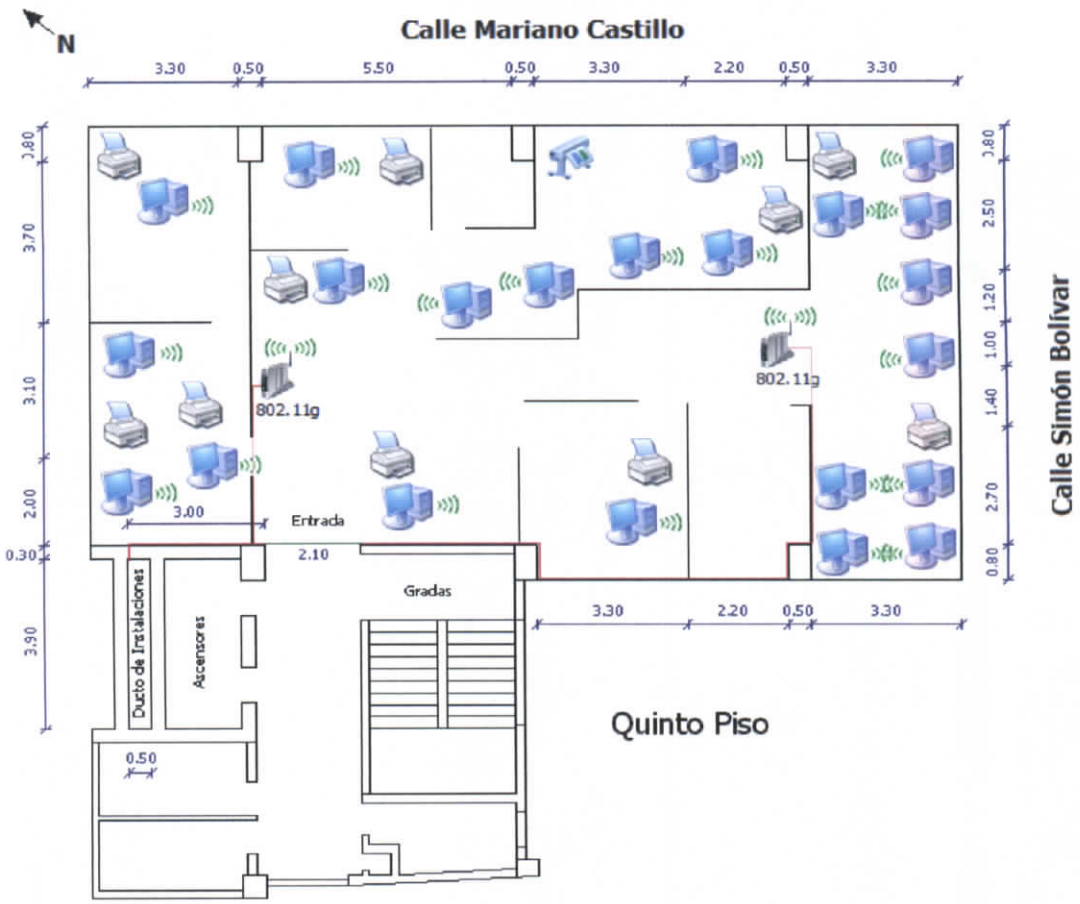


Figura 37: Vista del quinto piso del HCPT

Equipos	Conexión	SSID
2 Access Point	54 Mbps, 2.4GHz	HCPT_PLAN_G1 HCPT_PRO_G1
22 PC	802.11g 54Mbps	11 HCPT_PLAN_G1 11 HCPT_PRO_G1
Total 24 IPs		

Tabla 17: Resumen de dispositivos de red del quinto piso

Sexto Piso: Dirección Administrativa y Sistemas

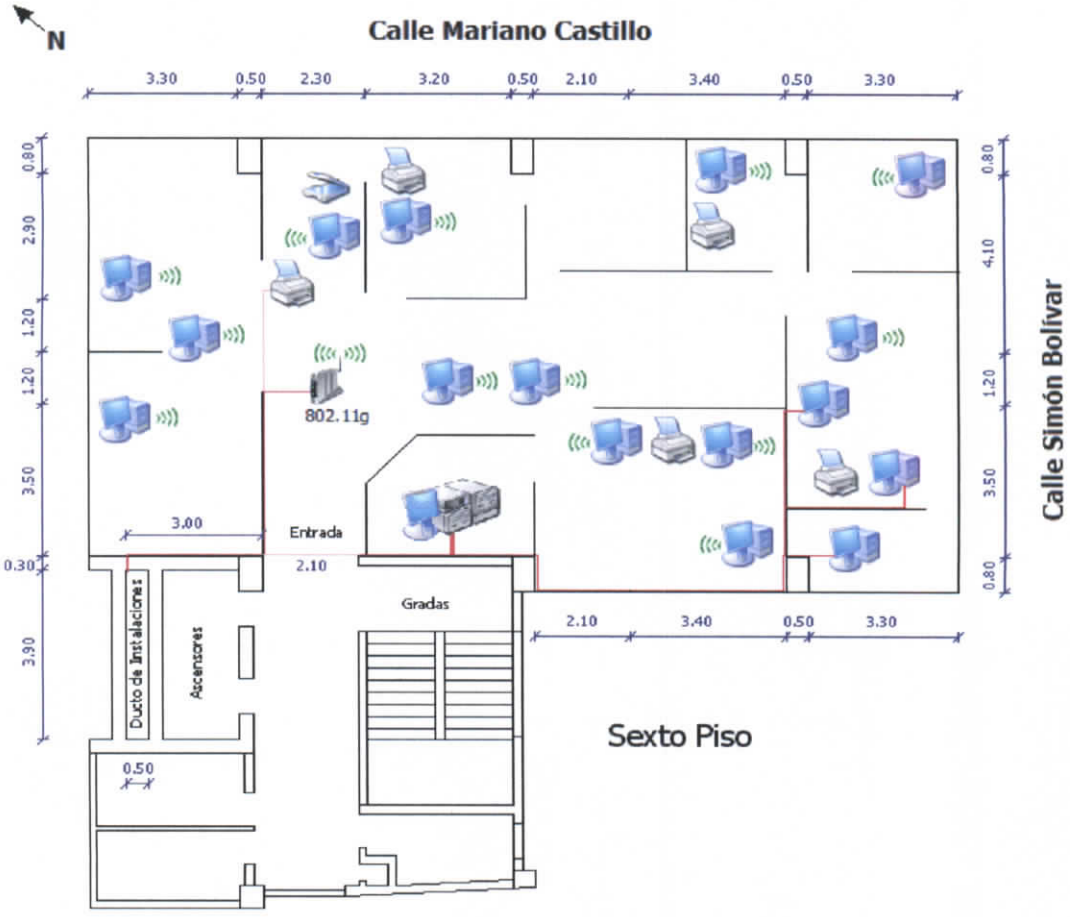


Figura 38: Vista del sexto piso del HCPT

Equipos	Conexión	SSID
1 Access Point	54 Mbps, 2.4GHz	HCPT_ADM_G1
13 PC	802.11g 54Mbps	13 HCPT_ADM_G1
3 PC	FastEthernet 100 Mbps	
1 Impresora Copiadora	FastEthernet 100 Mbps	
1 Firewall	FastEthernet 100 Mbps	
4 Servidores	GigabitEthernet 1000 Mbps	
Total 23 IPs		

Tabla 18: Resumen de dispositivos de red del sexto piso

Terraza del H. Consejo Provincial de Tungurahua: Antenas de Conexión de Spread Spectrum de 2.4GHz

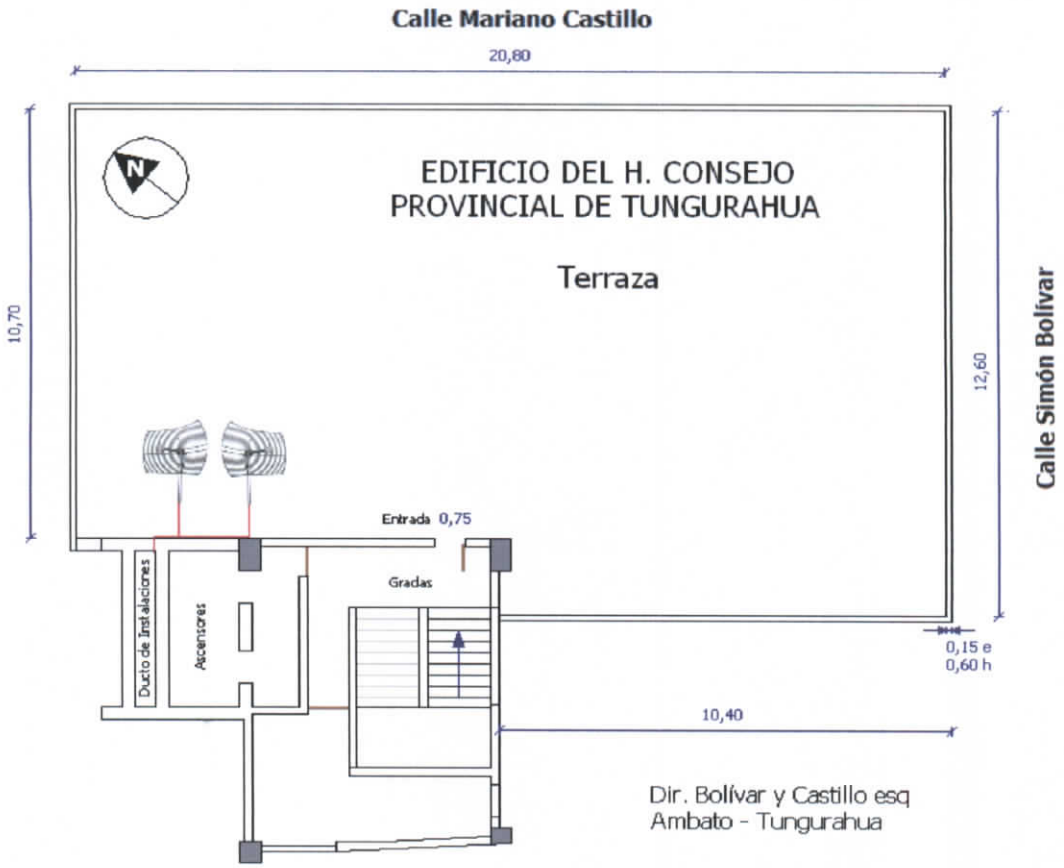


Figura 39: Vista de la terraza del HCPT

Equipos	Conexión	SSID
2 Radios Enlaces Spread Spectrum	10 Mbps, 2.4GHz	Extreme1 (Gobierno) Extreme2 (Talleres)
1 PC	802.11g 54Mbps	1 Extreme1
Total 3 IPs		

Tabla 19: Resumen de dispositivos de red de la terraza

Edificio de Centro de Promociones y Servicios de la Provincia: ubicado en las calles Juan José de Sucre y Mariano Castillo.

Figura 40: Edificio del Centro de Promociones y Servicio de la Provincia

Cableado Vertical

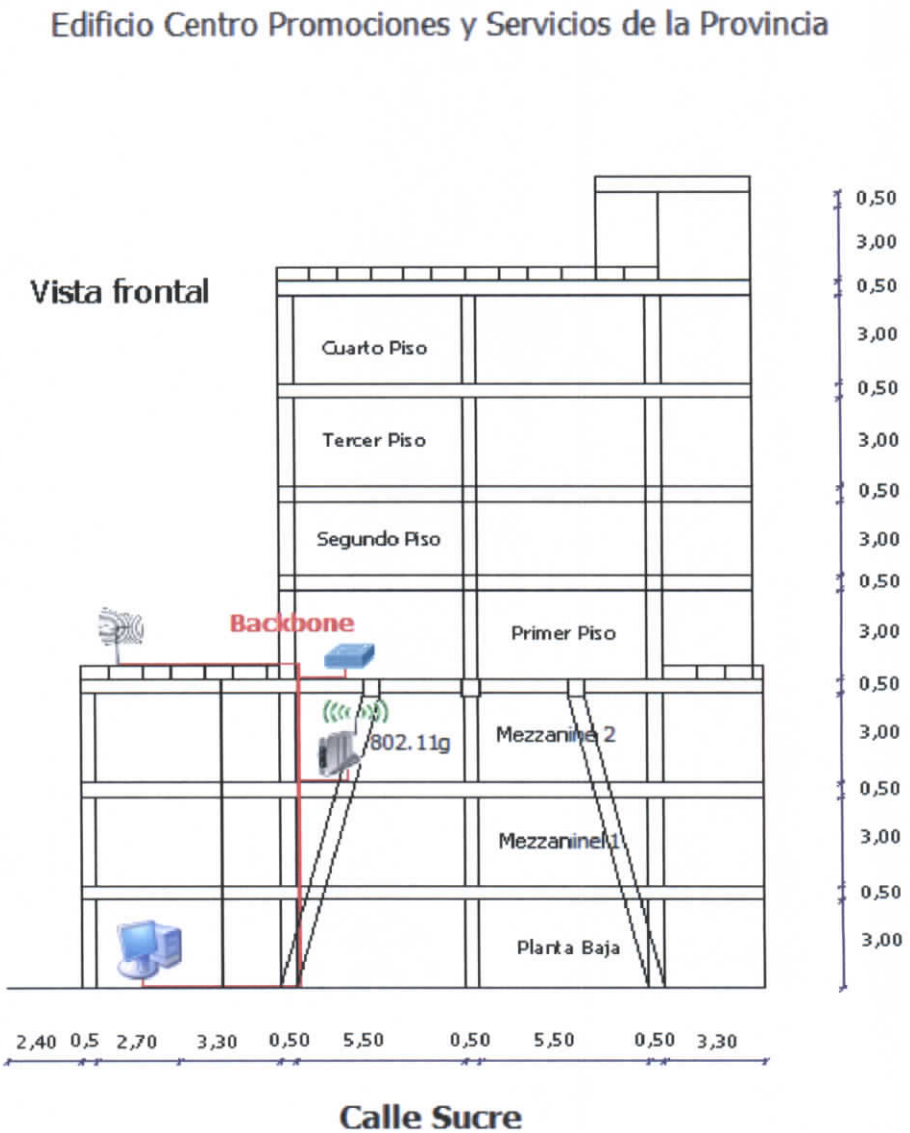


Figura 41: Cableado vertical del Gobierno Provincial

Cableado Horizontal

Planta Baja: Aula Virtual

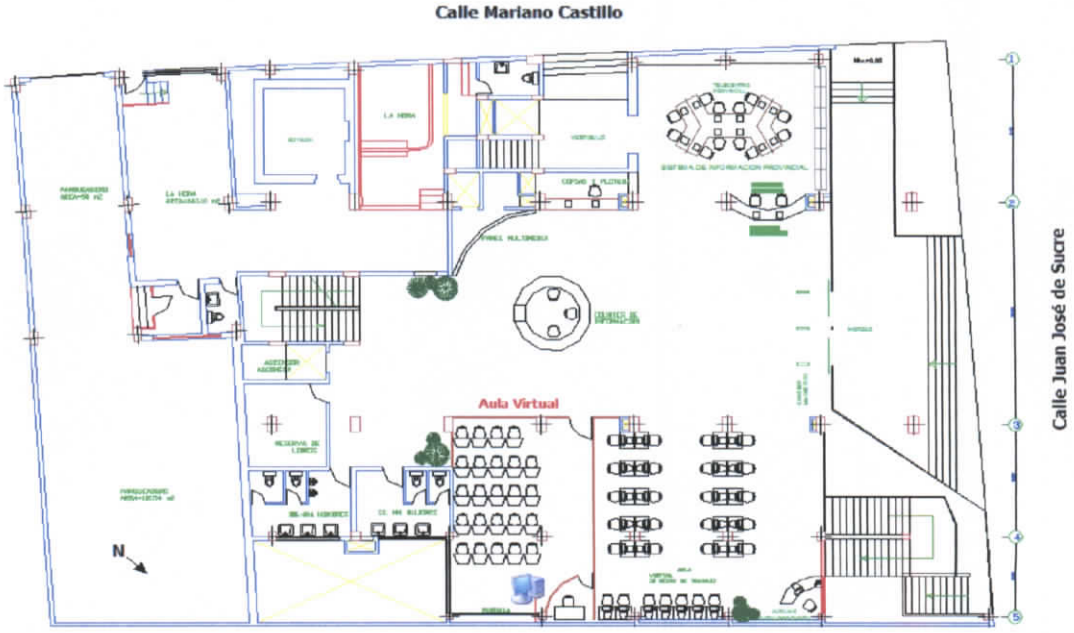


Figura 42: Vista de la planta baja del Centro de promociones y servicios de la provincia

Equipos	Conexión	Observaciones
1 PC	100 Mbps	
Total 1 IPs		

Tabla 20: Resumen de dispositivos de red de la planta baja del Centro de promociones y servicios de la provincia

Primer Mezzanine: Biblioteca I. Municipio de Ambato

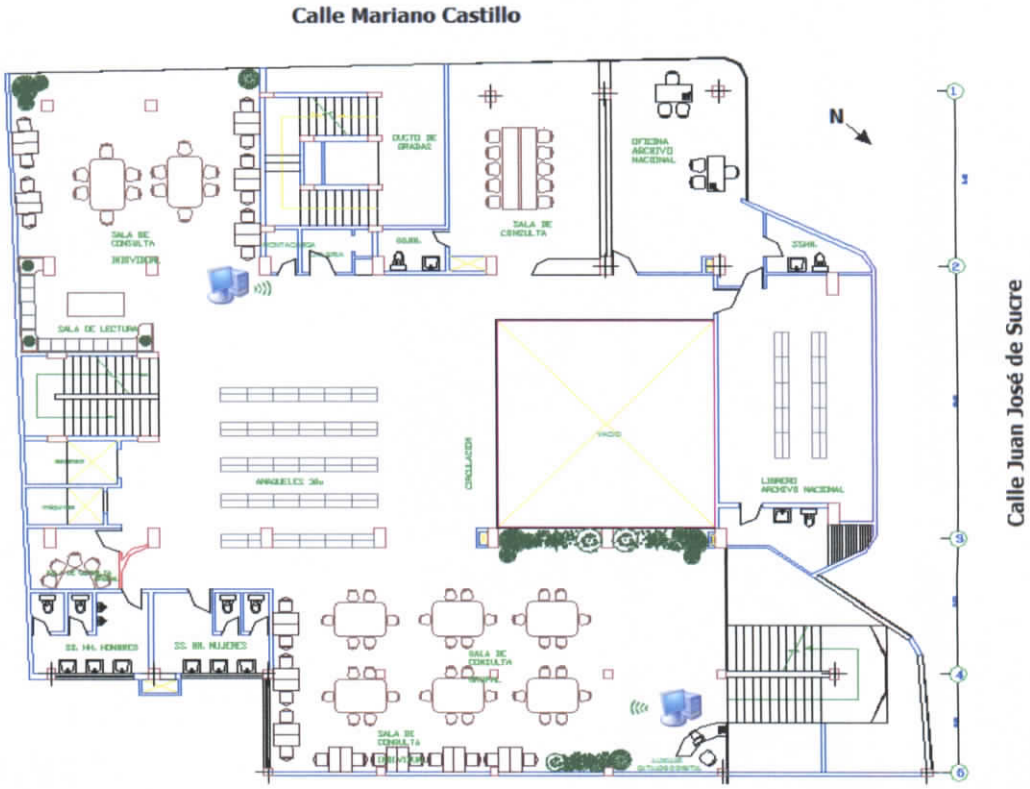


Figura 43: Vista del primer Mezzanine del Centro de promociones y servicios de la provincia

Equipos	Conexión	SSID
2 PC	802.11g 54Mbps	HCPT_BIB_G1
Total 2 IPs		

Tabla 21: Resumen de dispositivos del primer mezzanine del Centro de promociones y servicios de la provincia

Segundo Mezzanine: Biblioteca H. Consejo Provincial de Tungurahua

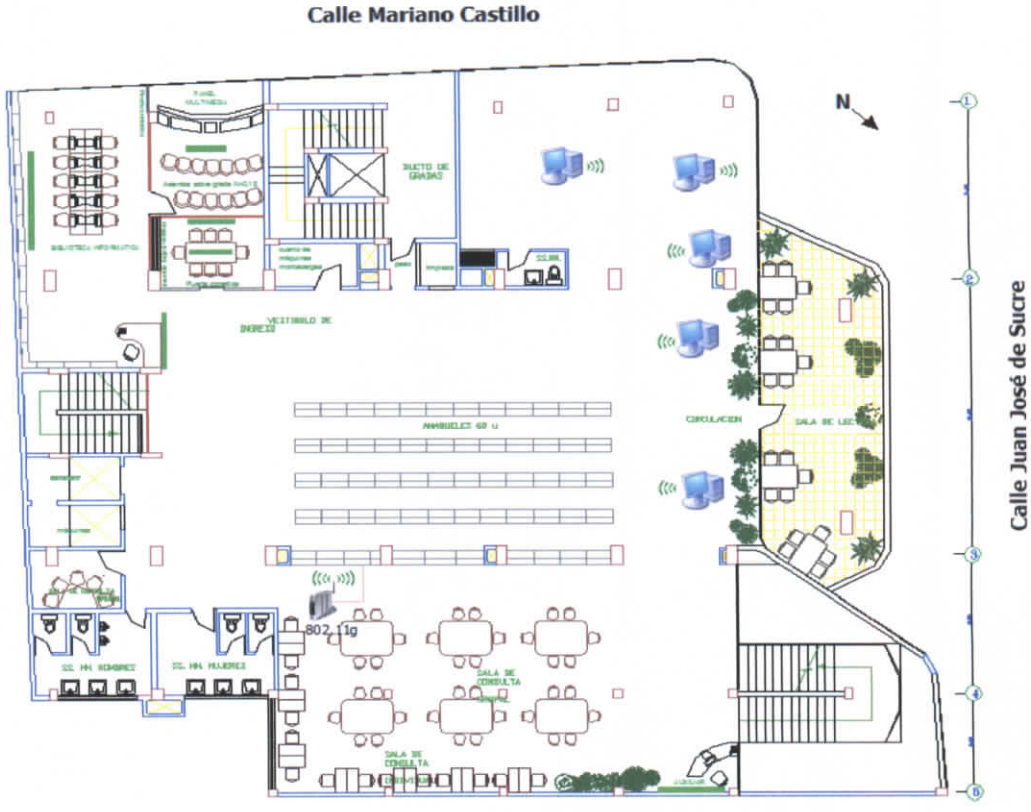


Figura 44: Vista del segundo mezzanine del Centro de promociones y servicios de la provincia

Equipos	Conexión	SSID
1 Access Point	54 Mbps	HCPT_BIB_G1
5 PC	802.11g 54Mbps	HCPT_BIB_G1
Total 6 IPs		

Tabla 22: Resumen de dispositivos de red del segundo mezzanine del Centro de promociones y servicios de la provincia

Primer Piso: Gobierno Provincial de Tungurahua

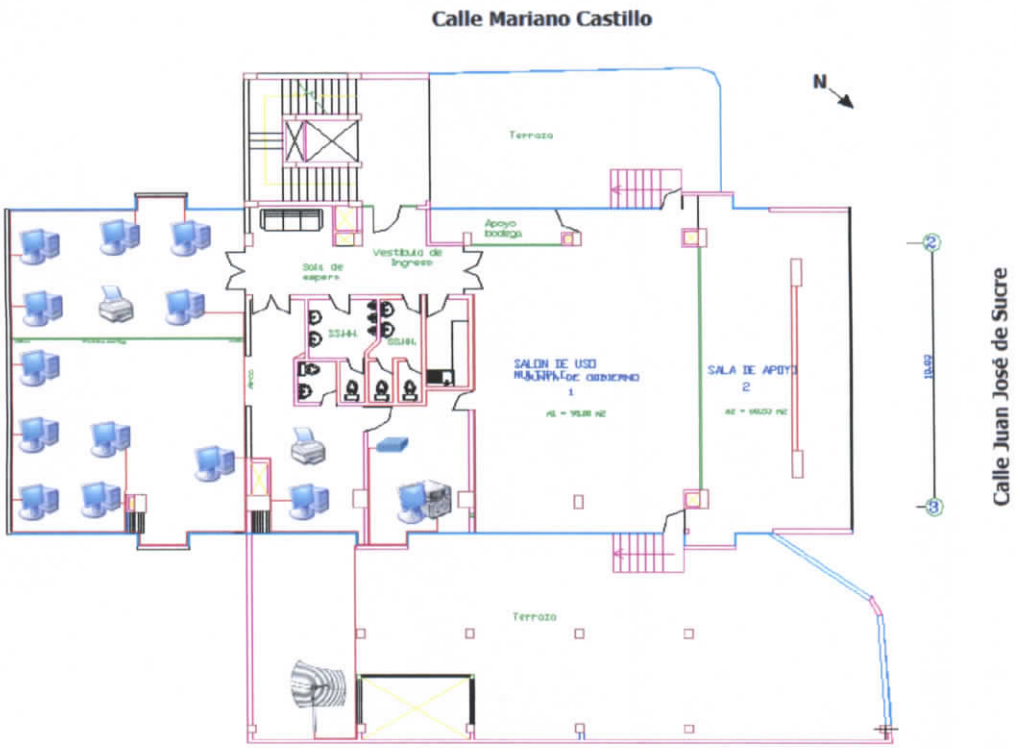


Figura 45: Vista del primer piso del Centro de promociones y servicios de la provincia

Equipos	Conexión	SSID
1 Radios Enlaces Speed Spectrum	10 Mbps, 2.4GHz	Extreme1 (HCPT-Gobierno)
12 PC	100 Mbps	
1 Servidor	1000 Mbps	
2 Impresoras en Red	100 Mbps	
Total 16 IPs		

Tabla 23: Resumen de dispositivos de red del primer piso del Centro de promociones y servicios de la provincia

Área de Bodega y Talleres del H. Consejo Provincial de Tungurahua: ubicado en las Avenidas González Suárez, Avenida de las Américas y Avenida Pedro Fermín Cevallos.

Figura 46: Área de Bodegas y Talleres del HCPT

Figura 47: Edificio del Sindicato de trabajadores del HCPT

Conexión Vertical

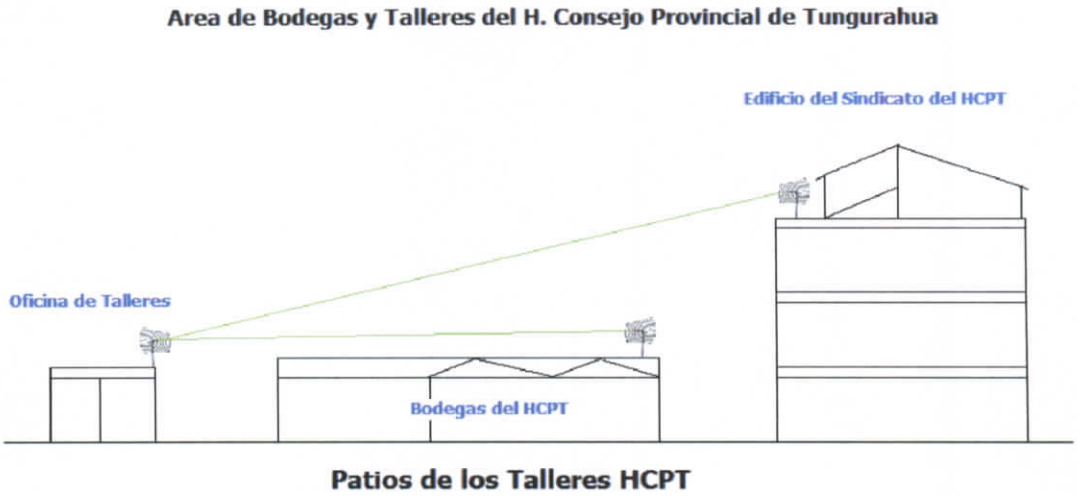


Figura 48: Vista frontal del Área de Bodega y Talleres

Conexión Horizontal

Área de Talleres del HCPT: Antenas de Conexión de Spread Spectrum de 2.4GHz

Figura 49: Vista de área de talleres y bodega del HCPT

Equipos	Conexión	SSID
1 Radios Enlaces Speed Sprectrum	10 Mbps, 2.4GHz	Extreme2 (HCPT-Talleres)
3 Access Point Bridge	802.11b 10Mbps	HCPT_BOD_B1
Total 4 IPs		

Tabla 24: Resumen de dispositivos de red del área de talleres y bodega

Oficina de Talleres

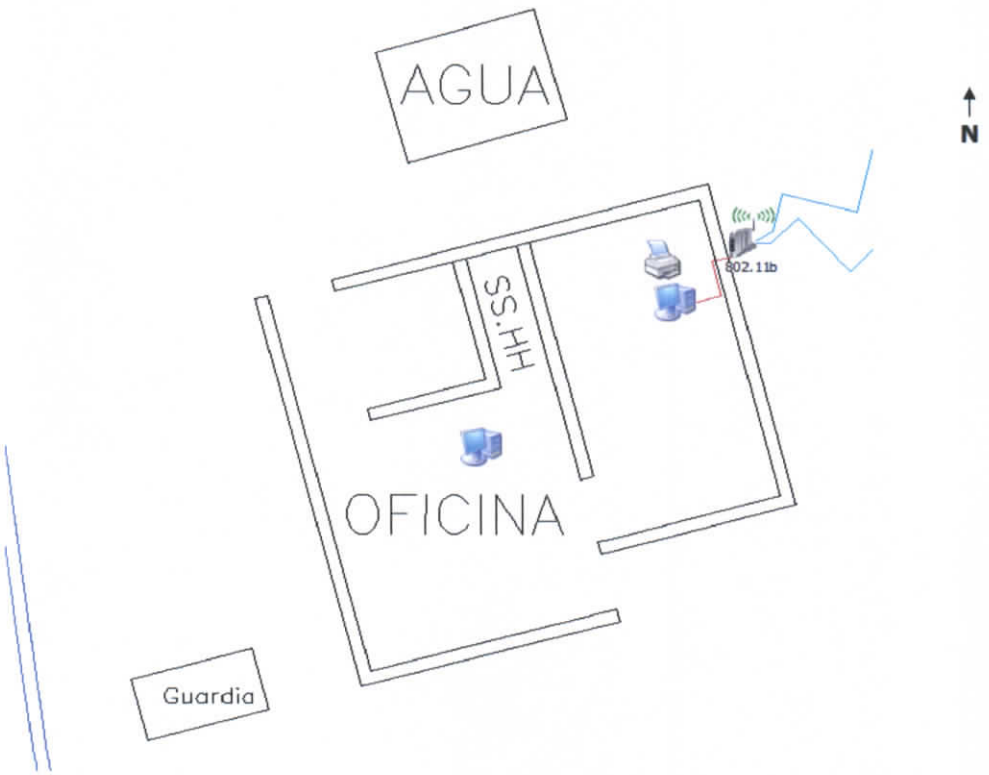


Figura 50: Vista de la oficina de talleres

Equipos	Conexión	Observaciones
1 PC con conexión directa	100 Mbps	Conectado al Access Point Externo
1 PC sin red		
Total 2 IPs		

Tabla 25: Resumen de dispositivos de red de la oficina de talleres

Oficina de Bodega

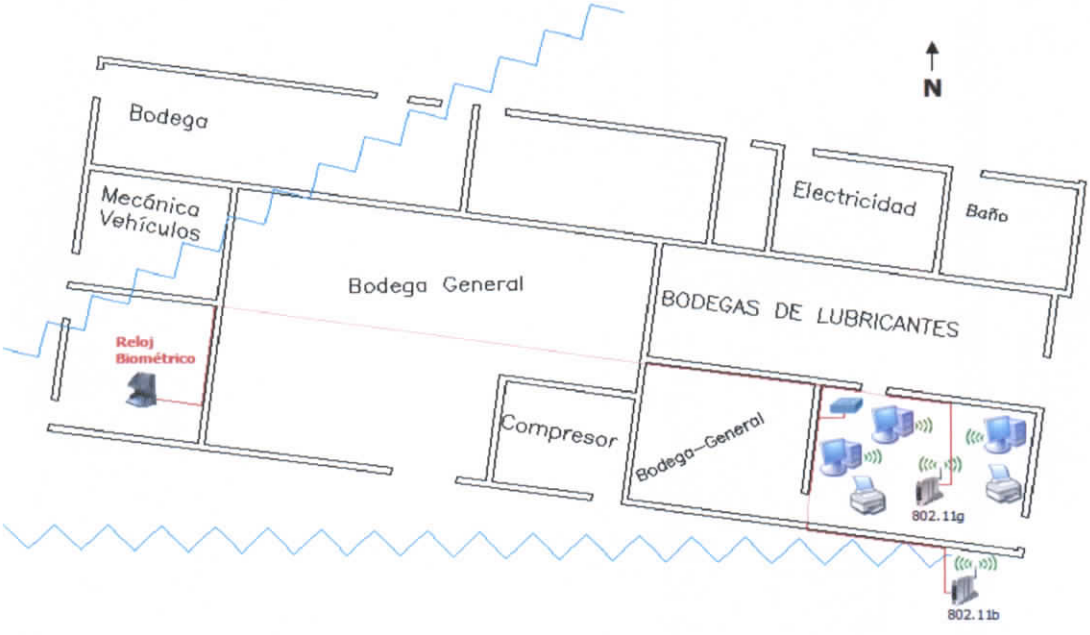


Figura 51: Vista de la oficina de bodega

Equipos	Conexión	SSID
1 Access Point	802.11g 54Mbps	HCPT_BOD_G1
3 PC	802.11g 54Mbps	HCPT_BOD_G1
1 Reloj Biométrico	10 MBPS	
Total 5 IPs		

Tabla 26: Resumen de dispositivos de red de la oficina de talleres

A continuación se presenta un diagrama lógico la interconexión de toda la red del H. Consejo Provincial de Tungurahua, que se representa como una topología de Estrella Extendida, y también se ofrece en una ampliación en el Anexo 7:

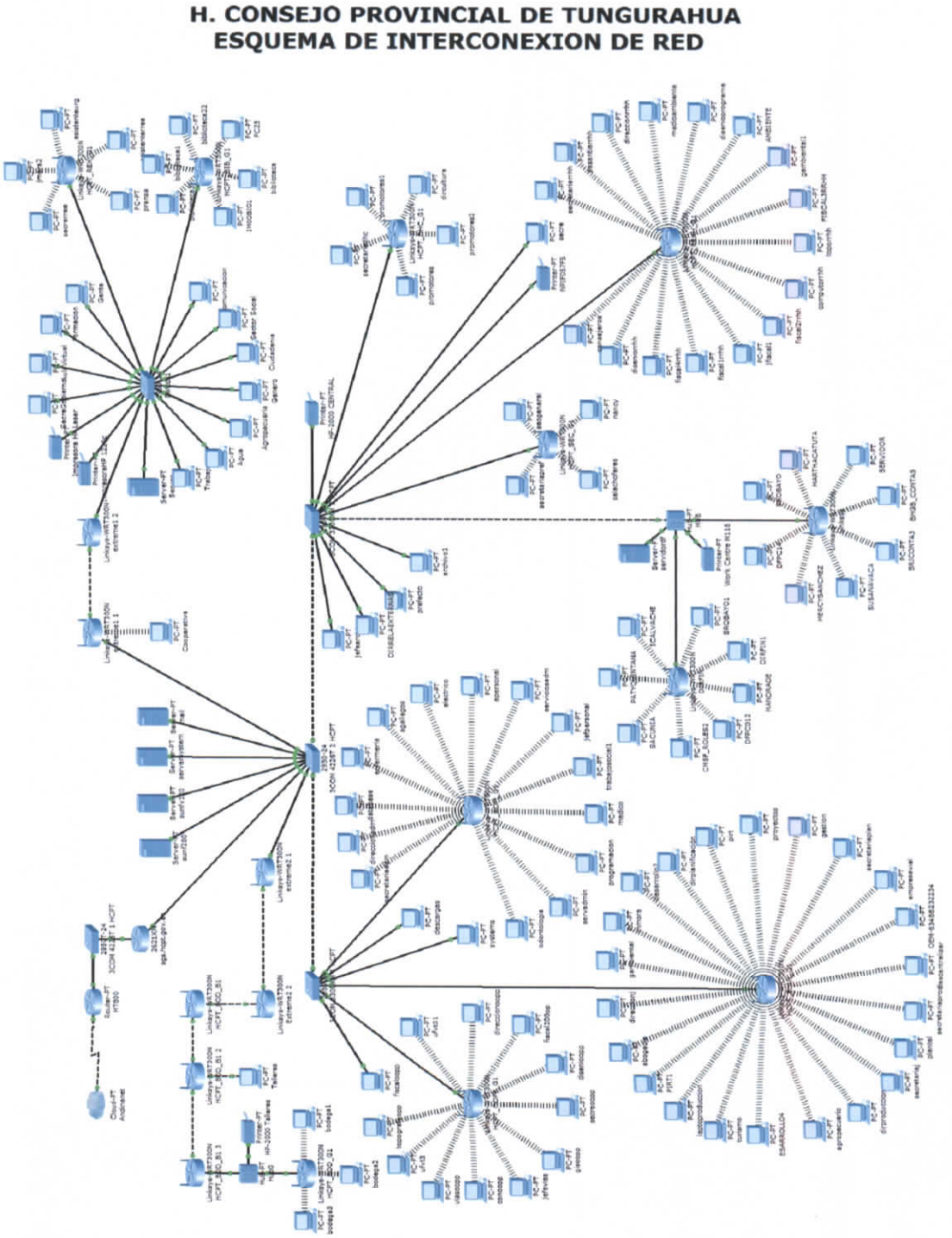


Figura 52: Esquema de conexión global de la red del HCPT

Resumen de Dispositivos Físicos

No	Dispositivo	Cantidad	Descripción
1	Servidores	6	Internet, Correo Electrónico, Base de Datos, Respaldo y Sistema Financiero
2	Computadores	105	Computadores conectados de manera inalámbrica
		21	Computadores conectados con cable de red categoría 5
3	Firewall	1	Dispositivo de seguridad de internet a nivel de datos
4	Switch Cisco Catalyst 3560G-48PS	1	Equipo especial para el Núcleo de la Red
5	Conmutadores 2 Switch 3COM 4226T 2 Switch 3COM 3300XM	4	Equipos de interconexión de red en la capa de distribución
6	Switch Hub	3	Equipos de comunicación de red para ampliar puntos de red
7	Access Points Inalámbricos	13	Puntos de acceso inalámbricos para la red
8	Enlaces de Espectro Ensanchado	7	Equipos para interconectar las dependencias de Bodega, Talleres y Centro de Promociones y Servicios
9	Puntos Impresoras	5	Puntos de Impresión de red que se tiene actualmente
10	Reloj Biométrico	2	Equipos para el control de ingreso de empleados y trabajadores
11	Modem ADSL MT800	1	Modem de conexión a internet ancho de banda 10024/512 Kbps
12	Laptops	4	Computadoras portátiles
13	Sistema de seguridad	1	Sistema de control de circuito cerrado de cámaras de vídeo para seguridad
	Total Dispositivos	**174**	**Dispositivos de red**

Tabla 27: Resumen General de dispositivos de red

3.5. Servicios y aplicaciones activas

Actualmente se encuentran en ejecución los siguientes Servicios y Aplicaciones que utilizan la infraestructura de la red para su ejecución y normal desarrollo de sus actividades.

Servicio	Servidor	Plataforma Servidor	Plataforma Clientes
Firewall	Symantec Gateway Security	Linux	
Internet Compartido	Squid 2.78	Solaris 9	Windows 98, Me,2000, XP, Vista
Correo electrónico	Lotus Domino 7.01	Solaris 9	Windows 98, Me,2000, XP, Vista, Lotus Notes8
Antivirus	Symantec EndPoint Protection 11	Windows 2003 Enterprise	Windows 98, Me,2000, XP, Vista
Controlador de Dominio	Active Directory	Windows 2003 Enterprise	Windows 98, Me,2000, XP, Vista
DNS	DNS Server	Windows 2003 Enterprise	Windows 98, Me,2000, XP, Vista
Adquisición de Materiales	base datos documentales de Lotus Domino	Solaris 9	Windows 98, Me,2000, XP, Vista, Lotus Notes 8
Sistema de Control de Recursos Humanos	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	Windows 98, Me,2000, XP, Vista, Clientes de la aplicación y Oracle
Sistema Médico Odontológico	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	Windows 98, Me,2000, XP, Vista, Clientes de la aplicación y Oracle
Sistema de Control de Proveedores	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	Windows 98, Me,2000, XP, Vista, Clientes de la aplicación y Oracle
Sistema Financiero FINANSG	Aplicación en Visual FOX 6 con base de datos de SQL 200 Server	Windows 2000 Advanced Server	Windows 98, Me,2000, XP, Vista, Cliente de la aplicación

Tabla 28: Resumen de servicios y aplicaciones

Del análisis realizado, se han detectado ciertos servicios de aplicación que se deben implementar en el HCPT

Por implementar

- Sistema de Administración de Trámites y Solicitudes
- Sistema de Control de Combustibles
- Sistema de Control de bienes e inventario
- Sistema de Administración y Control de Soporte y Mantenimiento de Equipos
- Sistema de Administración y Control de Contratos y Obras
- Sistema de Precios Unitarios y Presupuestos
- Sistema de Mapas Virtuales

3.6. Análisis del tráfico de la red actual

Para esto se utilizó la herramienta Wireshark que permite capturar paquetes de red, con el fin de analizar el flujo de información y determinar los diferentes servicios de red que están siendo utilizados, los datos que se obtienen son: la fecha y hora de la ocurrencia, las direcciones IP de origen y destino, el protocolo que se utilizó y la información de tráfico de los paquetes.

Pantalla de captura del Wireshark v 1.0.1

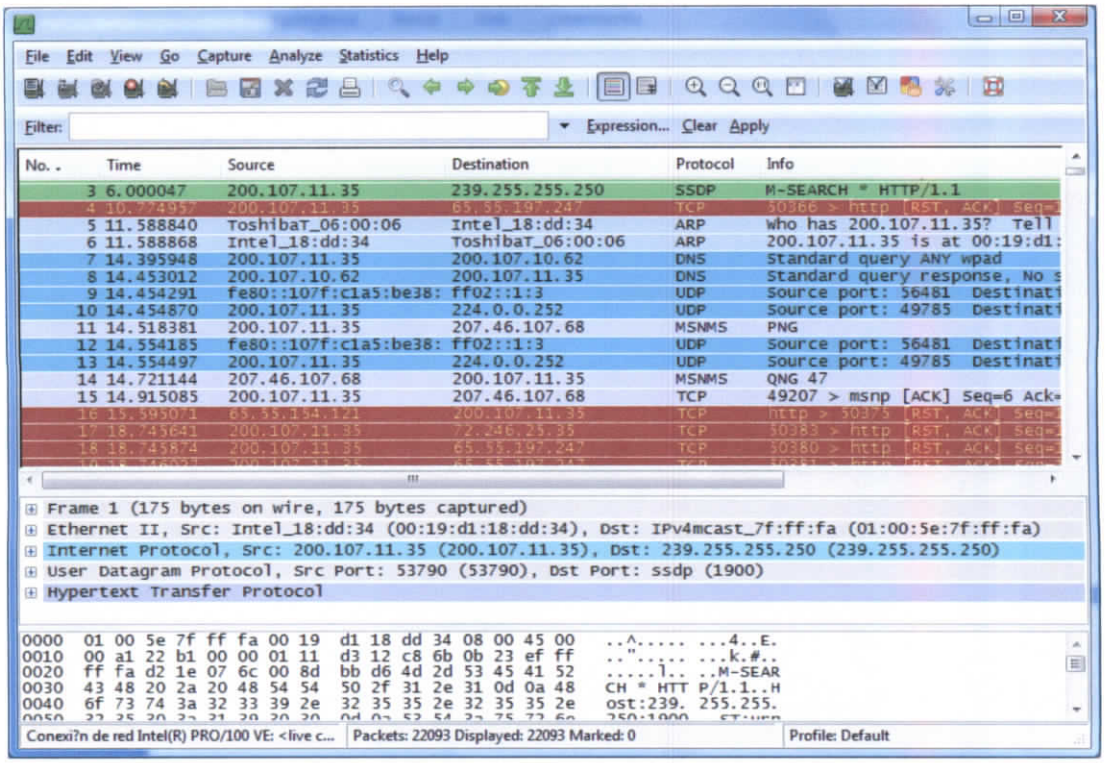


Figura 53: Programa Wireshark

Con la ayuda de esta herramienta se realizaron varias capturas durante la última semana del mes de mayo, la razón fue porque en esa semana por ser fin de mes, siempre existe mayor movimiento de peticiones, facturación, consultas, pagos y transferencias en línea, de lo cual a continuación se muestra las capturas más significativas con su respectivo análisis.

1. Se utilizó un periodo de una hora del día lunes en la mañana entre 9 a 10 de la última semana del mes de mayo.

Se obtuvo el siguiente resumen de tráfico de red con el listado de los protocolos existentes

Protocolo	Ocurrencias	Porcentaje
TCP	322518	40%
ARP	188301	27%
SMTP	142328	20%
SSDP	8838	2%
DNS	7419	2%
IGMP	5362	2%
Gnutella	4610	2%
Messenger	4066	1%
HTTP	3789	1%
BitTorrent	3012	1%
NBNS	2841	0%
BROWSER	1723	0%
UDP	797	0%
ICMP	623	0%
STP	461	0%
TLSv1	196	0%
UCP	4	0%
PKTC	3	0%
FC	3	0%
OICQ	3	0%
GTP	1	0%
FF	1	0%
H1	1	0%
Total general	**696900**	

Tabla 29: Tráfico de red 1

Representación gráfica en pastel del porcentaje de incidencia del tráfico de red.

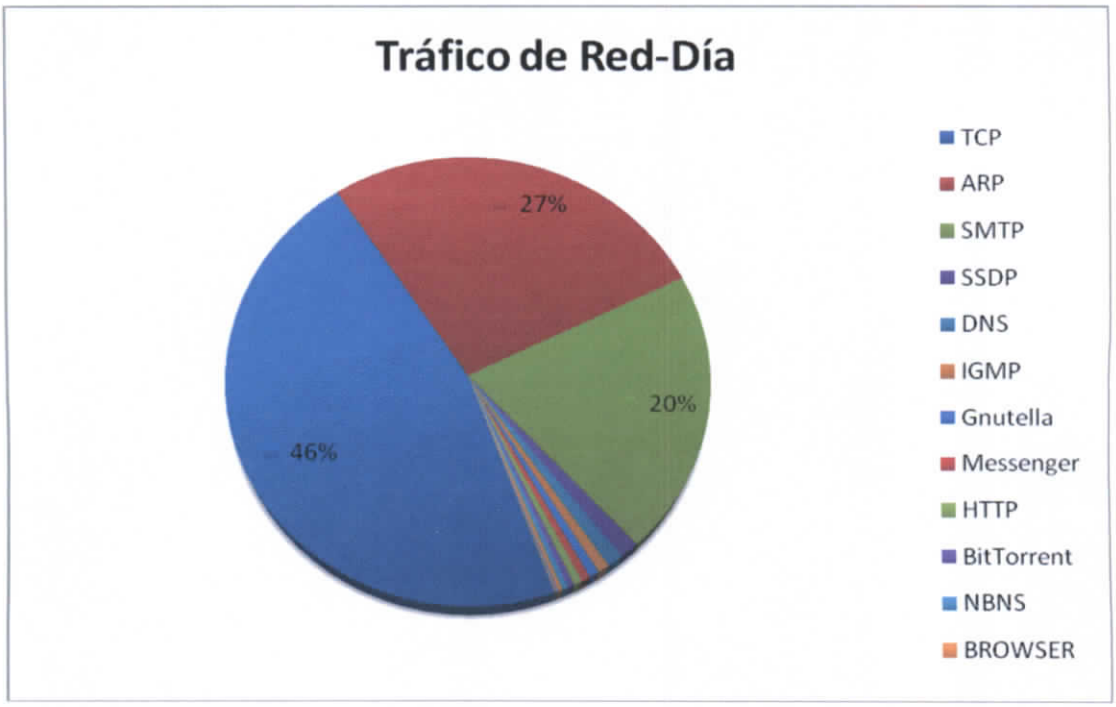


Figura 54: Tráfico de red de un día

De la gráfica se puede apreciar que el servicio de Broadcast ocupa casi la tercera parte de todo el tráfico y el servicio de correo tiene un porcentaje alto que indica que puede estar siendo atacado por Spam.

2. La siguiente captura representa a un conjunto o agrupación de datos tomados de lunes a viernes a la misma hora; es decir, entre 9 a 10 de la mañana y combinado en un solo archivo de análisis

Se obtuvo el siguiente resumen de tráfico de red con el listado de los protocolos más representativos

Protocolo	Ocurrencias	Porcentaje
ARP	1472835	40%
SMTP	517450	14%
TCP	503115	14%
HTTP	328520	9%
FTP-DATA	302640	8%
SMB	174140	5%
STP	151870	4%
NBNS	86885	2%
MS NLB	76130	2%
ICMP	38605	1%
LOOP	30650	1%
DNS	15655	0%
BROWSER	13060	0%
Total general	**3711555**	

Tabla 30: Tráfico de red

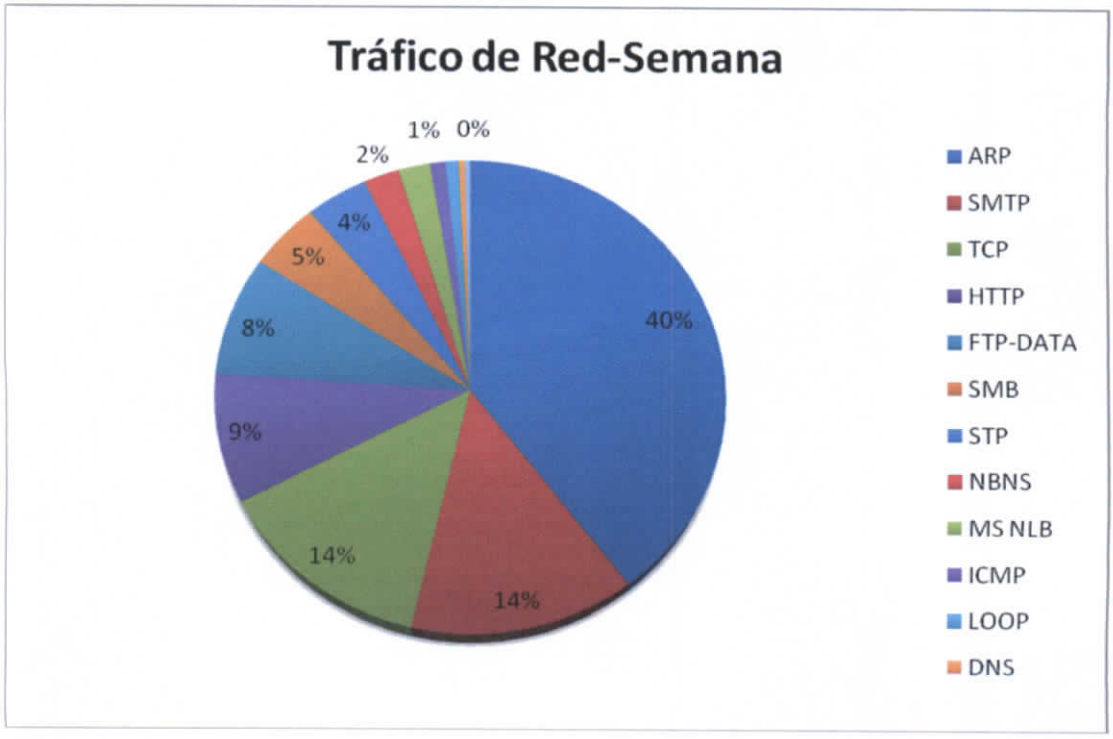


Figura 55: Tráfico de red de semana

De lo cual se tiene que el tráfico de broadcast ocupa la mayor parte deduciendo que todas las consultas de broadcast que se realizan se

difunden por toda la infraestructura de red e incluso llegan a los sitios remotos, esto se da porque la estructura lógica de la red es plana del tipo 192.168.1.0/254

El SMTP también indica que hay mucho tráfico por lo que podría ser considerado en su mayoría como correo basura.

3.7. Análisis de la seguridad actual

Partiremos primero haciendo una revisión de los siguientes aspectos

3.7.1. Defensa contra Amenazas

3.7.1.1. Protección antivirus

Actualmente el HCPT tiene una solución empresarial Symantec Endpoint 11 que es administrable, configurable y permite monitorear, controlar a los clientes así como también difundir las actualizaciones automáticas a los clientes.

Los servicios que se configuran en el servidor son:

- Antivirus y Antispyware
- Cortafuegos
- Prevención de intrusiones
- Control de Aplicaciones y dispositivos
- Actualizaciones automáticas
- Excepciones

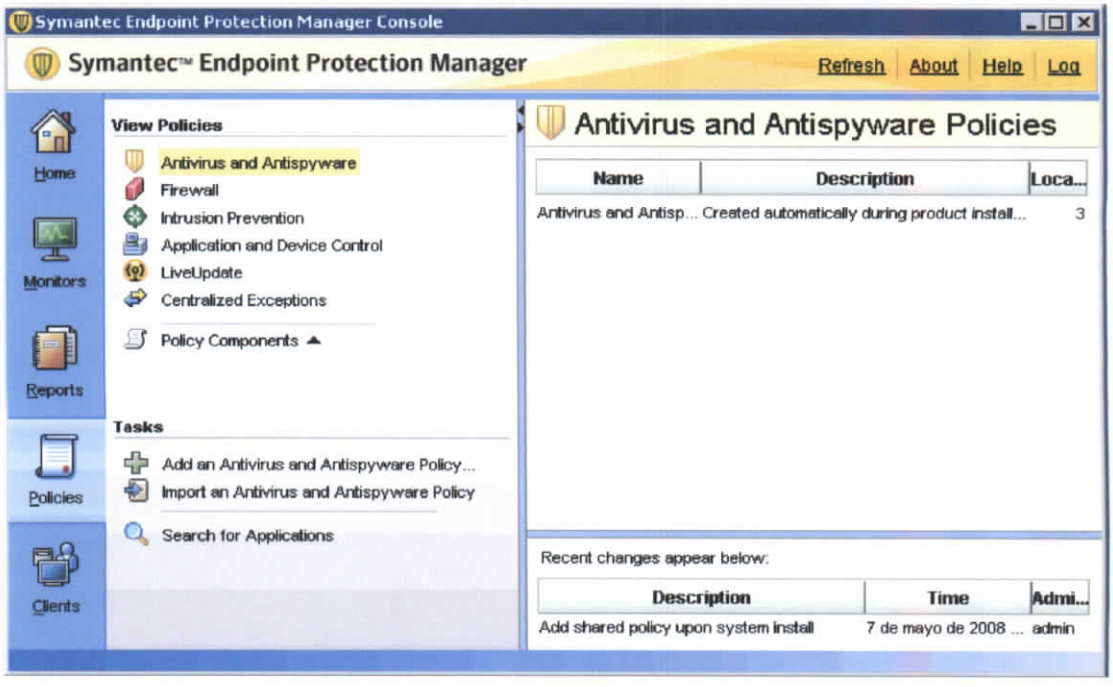


Figura 56: Symantec Endpoint Protection Manager Console

Para los clientes antivirus los servicios que se indican son los siguientes:

- Antivirus y Antispyware
- Protección contra amenazas proactivas
- Protección contra amenazas de red

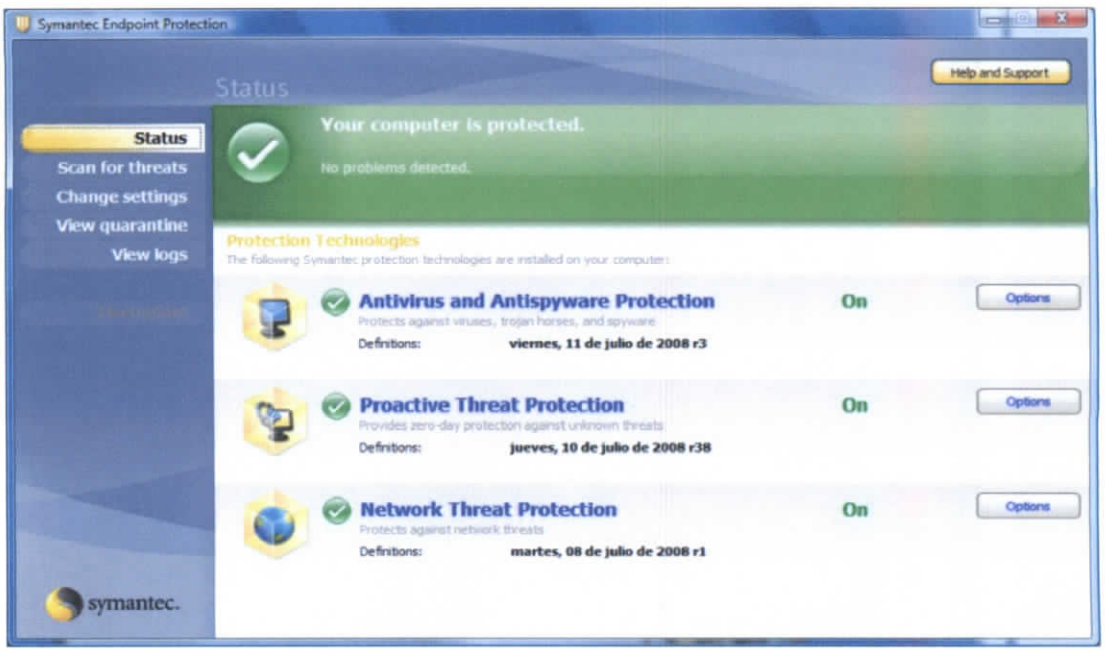


Figura 57: Symantec Endpoint Protection

3.7.1.2. Filtrado de paquetes

No se dispone de ninguna regla o programa que filtre paquetes de red a nivel de Switch, firewall o servidores

3.7.1.3. Detección y prevención de intrusiones

Se dispone de un equipo firewall Symantec Gateway Security 1600 Series que administra los servicios de Antivirus, Antispam, filtrado de contenido, detección y prevención de intrusiones, así como también a nivel de software antivirus Symantec Endpoint Protection como se muestra en la figura 35.

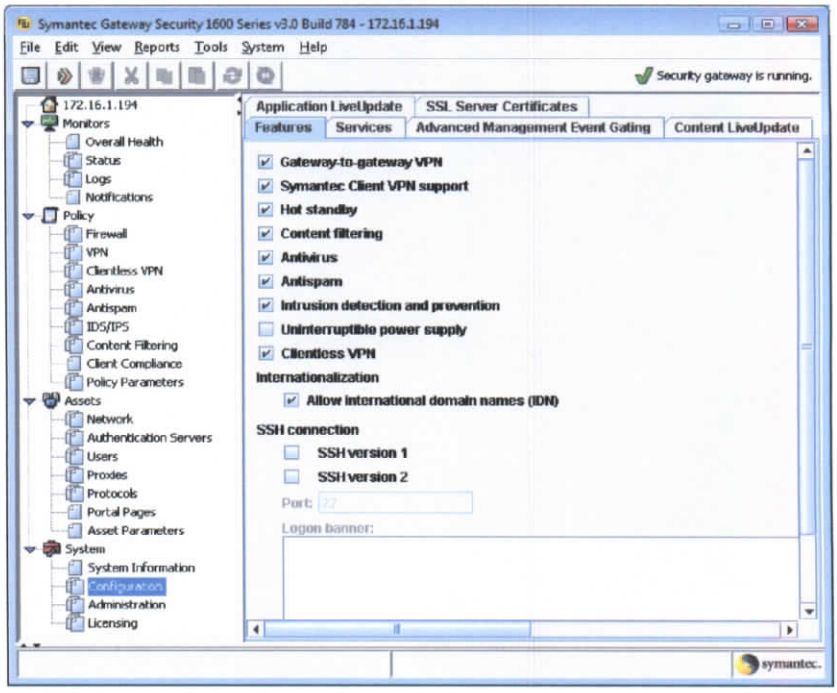


Figura 58: Symantec Gateway Security 1600 Series – Servicios

Actualmente el dispositivo firewall no tiene actualizada las licencias de: suscripción de antivirus y antispam, suscripción de la Base de datos del filtrado de contenido y la subscripción de la base de datos de detección y prevención de intrusiones. Este equipo ya no tiene soporte por parte del fabricante, siendo una de las razones por la cual se puede ocasionar el suceso del Spam explicado en el análisis del tráfico de red.

Aquí se muestran, en la gráfica siguiente los servicios que han expirado y que necesitan ser tomados en cuenta para resolver los inconvenientes de protección contra amenazas externas, sean éstas por contenido, correo o comportamiento extraño de peticiones:

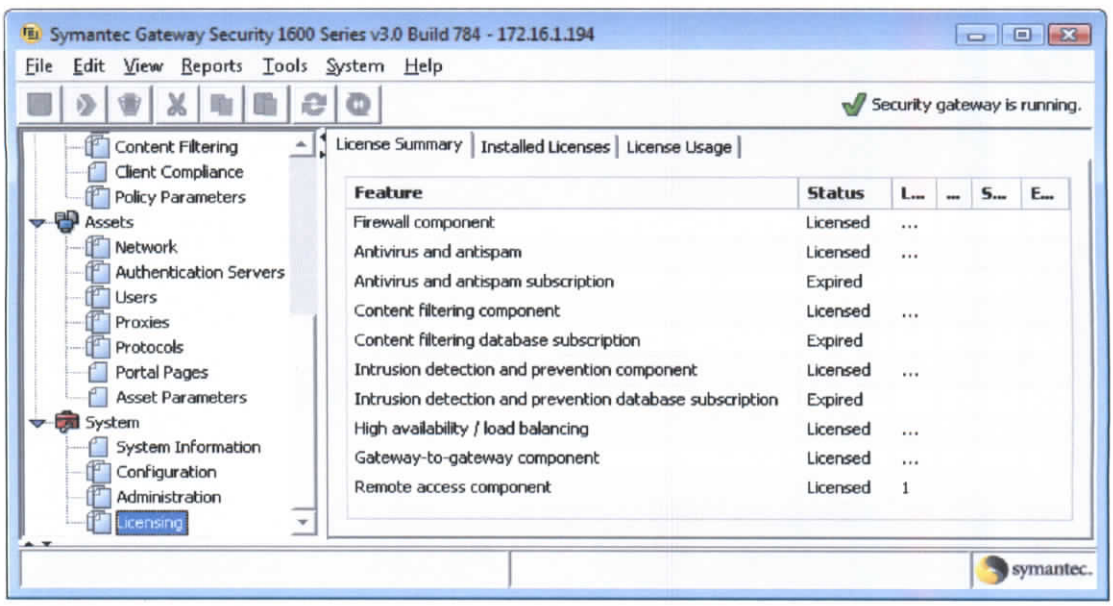


Figura 59: Symantec Gateway Security 1600 Series - Licencias Expiradas

3.7.1.4. Filtrado de contenidos

El equipo anterior Symantec Gateway Security 1600 Series, también incluye en sus características de protección los servicios de filtrado de contenido, pero también se ha personalizado en el Servidor Proxy de internet la aplicación squid v.26 para linux que permite restringir el acceso a contenido no apropiado y potencialmente peligroso y/o ofensivo, en el cual está configurado por listas de control de acceso y luego restricciones proxy, como se indica en las siguientes figuras:

Indice de Módulo
Ayuda..

Control de Acceso

Aplicar Cambios
Parar Squid

Listas de control de Acceso | Restricciones Proxy | Restricciones ICP | Programas externo

Nombre	Tipo	Coincidiendo con...
QUERY	Expresión Regular de Ruta URL	cgi-bin \?
apache		Server ^Apache
all	Dirección de Cliente	0.0.0.0/0.0.0.0
manager	Protocolo URL	cache_object
localhost	Dirección de Cliente	127.0.0.1/255.255.255.255
to_localhost	Dirección de Servidor Web	127.0.0.0/8
SSL_ports	Puerto URL	443 563
Safe_ports	Puerto URL	80
Safe_ports	Puerto URL	21
Safe_ports	Puerto URL	443 563
Safe_ports	Puerto URL	70
Safe_ports	Puerto URL	210
Safe_ports	Puerto URL	1025-65535
Safe_ports	Puerto URL	280
Safe_ports	Puerto URL	488
Safe_ports	Puerto URL	591
Safe_ports	Puerto URL	777
SSL_ports	Puerto URL	2083 2096
Safe_ports	Puerto URL	1443
CONNECT	Método de Petición	CONNECT
hcpt_net	Dirección de Cliente	172.16.0.0/255.255.254.0
permitidos	Dirección de Cliente	Desde archivo `/etc/squid/reglas/permitidos`
castigado	Dirección de Cliente	Desde archivo `/etc/squid/reglas/castigado`
porn	Expresión Regular URL	Desde archivo `/etc/squid/reglas/porn`
noporn	Expresión Regular URL	Desde archivo `/etc/squid/reglas/noporn`
contenidos	Expresión Regular de Ruta URL	Desde archivo `/etc/squid/reglas/contenidos`
horariom	Fecha y Hora	MTWHF 7:50-13:30
horariot	Fecha y Hora	MTWHF 14:00-21:00
sitiosp	Expresión Regular URL	Desde archivo `/etc/squid/reglas/sitiosp`
sigef	Puerto URL	8080

Figura 60: Lista de control de acceso

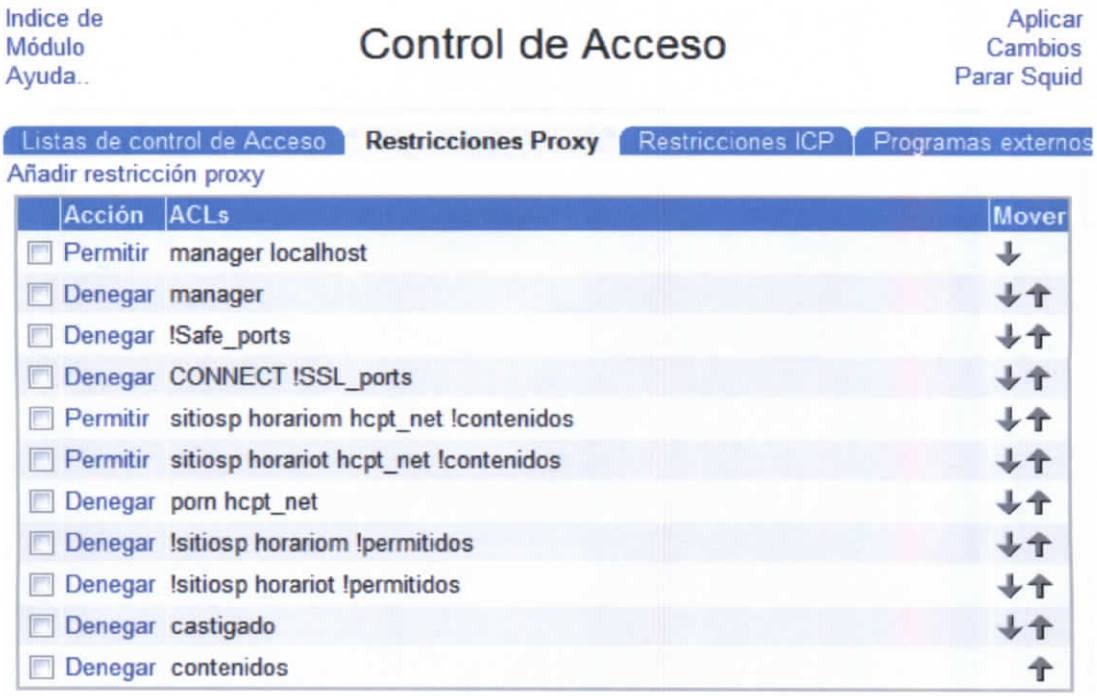


Figura 61: Restricciones proxy

3.7.2. Comunicación segura

Del análisis de situación actual se obtiene que no se dispone de ningún servicio de conexión a lugares remotos como para utilizar redes virtuales privadas VPN, por lo que este servicio no se utiliza al momento en el HCPT.

Tampoco se difunden servicios web para proveer de seguridad en línea con Secure Socket Layer (SSL)

Y no se utiliza un cifrado de archivos

3.7.3. La confianza y la identidad

Para esto se debe tomar en consideración los siguientes puntos:

3.7.3.1. Autenticación, autorización y cuentas (AAA)

Se dispone del software **Active directory** sobre la plataforma de Windows Server 2003 Enterprise, en el cual están creados los departamentos a nivel de Unidades Organizativas y dentro de éstas los usuarios que pertenecen a esas áreas.

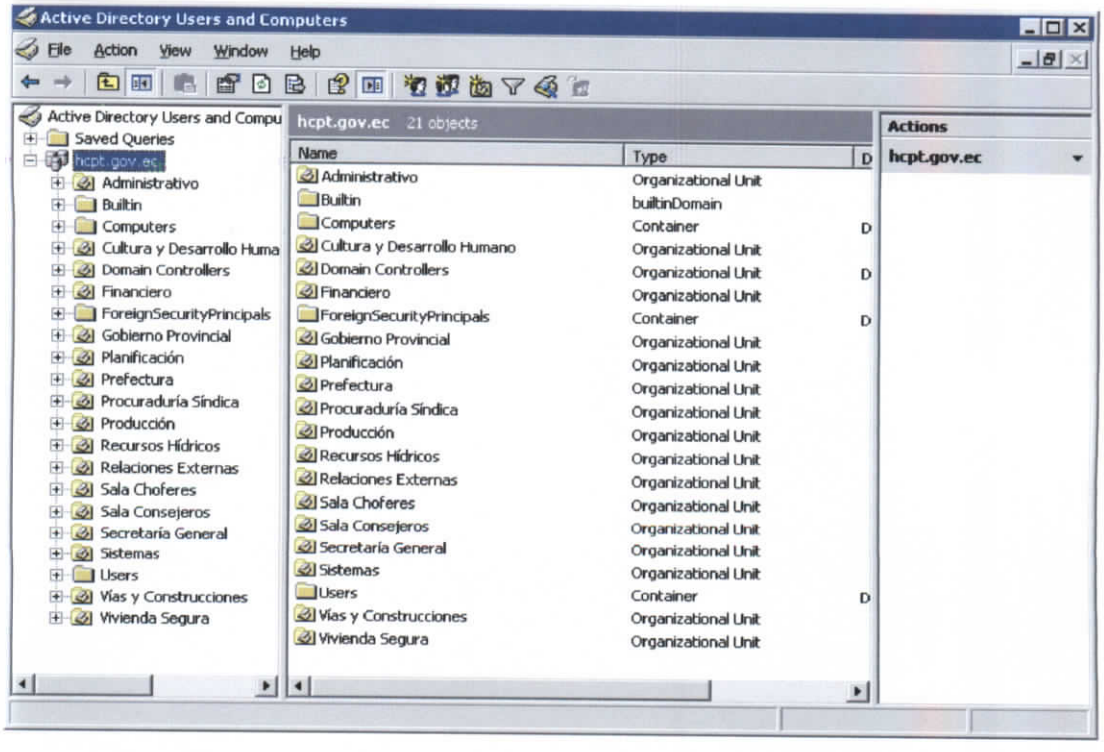


Figura 62: Active Directory Users and Computers

Para la parte de autenticación no se dispone de una política para el manejo de contraseñas, en vista de que ciertos usuarios no pueden memorizar claves complejas.

Para el control de acceso de equipos a la red wireless se tiene establecido por el filtrado de MAC Address, pero no se tiene ningún servidor de autenticación como RADIUS.

3.7.3.2. Control de admisión a la red (NAC)

Esta característica es administrada una parte por el sistema antivirus Symantec Endpoitn Protection.

3.7.3.3. Infraestructura de clave pública (PKI)

No se utiliza ningún sistema de administración y control de claves públicas

3.7.4. Puertos

También se ha determinado con la ayuda de software especializado (ip angry scan y ScanPorts) los puertos que están abiertos en cada uno de los dispositivos de red del HCPT, teniendo el siguiente resumen global:

Resumen de puertos abiertos en los dispositivos del HCPT

#	Descripción	Puerto	Cantidad	%
1	ECHO	7	1	0,14
2	Discard	9	1	0,14
3	Daytime	13	1	0,14
4	Quote	17	1	0,14
5	Chargen	19	1	0,14
6	FTP	21	137	19,2
7	Telnet	23	16	2,24
8	SMTP	25	137	19,2
9	WINS	42	1	0,14
10	DNS	53	4	0,56
11	HTTP	80	26	3,64
12	HTTP Lotus	81	1	0,14
13	Kerberos	88	2	0,28
14	POP3	110	138	19,3
15	Sunrpc	111	2	0,28
16	NNTP	119	4	0,56
17	epmap	135	61	8,53
18	NetBIOS Sesiones	139	73	10,2
19	LDAP	389	2	0,28
20	SilverPlatter	416	1	0,14
21	Onmux	417	1	0,14
22	HTTPS/SSL	443	7	0,98
23	Micosoft DS Active Directory	445	70	9,79
24	kpasswd	464	2	0,28
25	Ph service	481	1	0,14
26	exec	512	3	0,42
27	login	513	5	0,7
28	syslog	514	5	0,7
29	uucp.'uucpd'	540	1	0,14
30	RTSP	554	3	0,42
31	NNTPS	563	1	0,14
32	http-rpc-epmap	593	2	0,28
33	LDAPS	636	1	0,14
34	sun-manageconsole	898	1	0,14
35	Biometrico	1001	2	0,28

Tabla 31: Detalle de puertos abiertos

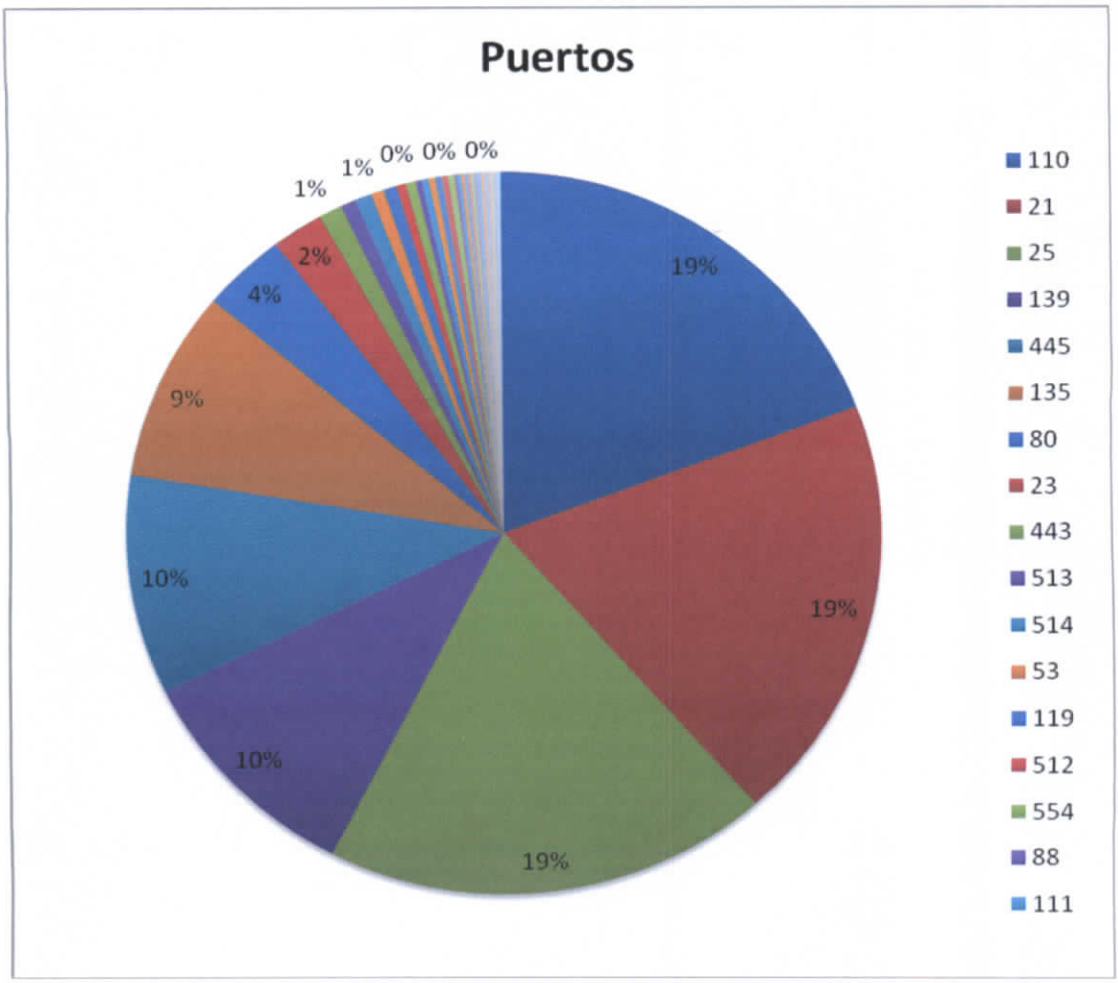


Figura 63: Porcentaje de puertos abiertos

De lo que se puede concluir que los puertos de FTP, POP3, SMTP, NETBIOS Sesiones y Micosoft DS Active Directory están activos en todas las computadoras

3.7.5. Respaldo de energía eléctrica

En la parte de suministro de energía eléctrica no se dispone de un sistema de protección y respaldo por lo que al momento de un apagón los equipos se apagan y pueden sufrir daños en sus circuitos electrónicos, únicamente se dispone de UPS de 1KVA para los servidores y para algunas estaciones de trabajo, pero el tiempo que se puede utilizar es de 15 minutos aproximadamente, por lo que en los fines de semana con un apagón de largo tiempo, los servidores se apagan luego de este tiempo de corte ocasionando que las sesiones y procesos no sean correctamente terminados, y es potencial riesgo a que se dañen estos servidores.

3.7.6. Otros Factores de seguridad

- Los dispositivos como Access points, switchs, firewall y equipos de seguridad soportan el protocolo SNMP.

- Para los recursos de red como archivos y carpetas, cada usuario debe compartir su carpeta y activar la casilla de permitir la escritura y modificar sus datos, no posee un servidor de archivos y respaldos para la documentación.

- Del estudio realizado se determina que no existe ninguna política de seguridad para el acceso, utilización, movimiento de los equipos y dispositivos en red ni para sus servicios.

3.8. Codificación, nomenclatura para denominación de equipos

Adicionalmente no existe una política de identificación de los dispositivos por lo que todos los computadores tienen los nombres de sus usuarios así como del departamento que laboran, es decir, hay una desorganización en la denominación o etiquetado de equipos, por lo que se ve la necesidad de dar una nomenclatura o codificación de equipos para un correcta administración.

3.9. Calidad de Servicio

Calidad de Servicio, en cada computador, todas las tarjetas de red tienen activado el protocolo de Programador de paquetes QoS, pero no dispone de configuraciones especiales en los dispositivos de comunicación que permitan llevar a cabo una buen distribución de tráfico de red, también no hay una clasificación del tráfico, por lo que sería partir realizando una clasificación de este tráfico y los servicios que se pretende tener a futuro como VozIP.

3.10. Resumen del análisis de situación actual

- Infraestructuras físicas conectadas a la red: Edificio Central, Centro de Promociones y Servicios de la Provincia, y Bodega y Talleres
- Equipos

Tipo	Cant.	Nombre	Descripción	Características	Servicios	Rend.
Swicth Capa 3	1	Cisco Catalyst 3560G-48PS	48 puertos	PoE		100%
Swicth Capa 2	2	3COM SuperStack 3 Switch 4226T	24 Puertos			100%
	2	3COM SuperStack 3 Switch 3300XM	24 Puertos			0%
Switch Capa 1	3	Hub Generic				100%
Servidores	1	Sunfirev120	Servidor Proxy de internet	Solaris 9	Squid-cache	0%
	1	SunFire280r	Servidor de Correo Elextrónico Interno	Solaris 9	Lotus Domino	90%
	1	SunFireV440	Servidor de Bases de Datos	Solaris 10	Oracle 10g	90%
	1	ServerHCPT	Servidor de Dominio, DNS y Antivirus	Windows 2003 Server Enterprise	Active Directory Symantec EndPoint Protection 11	90%
	1	ServidorDF	Servidor de Sistema Contable FINANSG	Windows 2000 Advanced Server	SQL Server 2000 FINANSG	50%
	1	ServidorHP	Servidor de Aplicación Mapeo de Actores	Linux Fedora 10	Sistema de Mapeo de Actores MySQL	50%
Firewall	1	Symantec Gateway Security	Protección		SPAM, IDS, Filtrado Contenidos	70%
Modem	1	Huawei SMARTAX MT 800	Conexión ADSL	1024/512		100%
Access Points	10	Proxim ORiNOCO® AP-4000	Access Point 802,11g, 2.4 GHz	MAC Filter	DCHP, VLANS	90%
	4	TEW-430APB 802.11g Wireless Access Point	Access Point 802,11g, 2.4 GHz	MAC Filter		75%
	3	Senao International NCB-8610	Access Point 802,11b 2.4 GHz	MAC Filter		80%
	2	Linksys WAP54G	Access Point 802,11g, 2.4 GHz	MAC Filter	2	100%

Tabla 32: Resumen de dispositivos de red

- Servicios

No.	Servidor	Aplicación	Sistema Operativo	Rend.
1	Firewall	Symantec Gateway Security	Linux	75%
2	Internet Compartido	Squid 2.78	Solaris 9	0%
3	Internet Compartido Provisional	Squid 2.78	Suse 10	100%
4	Correo electrónico	Lotus Domino 7.01	Solaris 9	90%
5	Antivirus Corporativo	Symantec EndPoint Protection 11	Windows 2003 Enterprise	100%
6	Controlador de Dominio	Active Directory	Windows 2003 Enterprise	100%
7	Domain Name Server	DNS Server	Windows 2003 Enterprise	100%
8	Adquisición de Materiales	base datos documentales de Lotus Domino	Solaris 9	100%
9	Sistema de Control de Recursos Humanos	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	95%
10	Sistema Médico Odontológico	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	25%
11	Sistema de Control de Proveedores	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	95%
12	Sistema Financiero FINANSG	Aplicación en Visual FOX 6 con base de datos de SQL 200 Server	Windows 2000 Advanced Server	95%

Tabla 33: Resumen de Servicios

- Políticas de Seguridad : NO

- Tráfico de red, protocolos más representativos

Tráfico	Protocolo	Porcentaje %
1	ARP	40
2	SMTP	14
3	TCP	14

Tabla 34: Resumen de Protocolos con mayor tráfico

- Seguridades

Nombre	Cantidad	Tipo	Servicio	Rend.
Defensa contra amenazas				
Antivirus	1	Software	Symantec Endpoint Protection 11	100%
	1	Hardware	Symantec Gateway Security 1600 Series	0%
AntiSpyware	1	Software	Symantec Endpoint Protection 11	100%
Antispam	1	Software	Symantec Endpoint Protection 11	100%
	1	Hardware	Symantec Gateway Security 1600 Series	0%
Filtrado de paquetes	No			
Detección y Prevencion de intrusiones	1	Software	Symantec Endpoint Protection 11	100%
	1	Hardware	Symantec Gateway Security 1600 Series	0%
Filtrado de contenido	1	Software	Squid 2.6	100%
	1	Hardware	Symantec Gateway Security 1600 Series	0%
Comunicación Segura				
VPN	No			
SSL	No			
Cifrado de archivos	No			
Confianza y la Identidad				
AAA	1	Software	Active directory	95%
NAC	1	Software	Symantec Endpoint Protect 11	75%
PKI	No			

Tabla 35: Resumen de Seguridades

- QoS: Ninguna Implementada

- Otras

- Ancho de Banda de internet: 1024/512 kbps
- Muchos puertos abiertos
- No se cuenta con sistema de respaldo de energía eléctrica

- Soporta IPV6
- Cableado estructurado categoría 5e
- No existe Redundancia
- Casi todas las dependencias tienen servicio de conexión inalámbrica 802,11g
- Seguridad inalámbrica WEP y filtrado de MAC address
- No hay VLANS la red es plana clase C la dirección de red es 192.168.1.0/24
- No existe Ruteo
- No existe una Codificación de equipos

CAPÍTULO IV

4. DISEÑO DE LA PROPUESTA TÉCNICA PARA EL FORTALECIMIENTO DE LA RED INFORMÁTICA DEL H. CONSEJO PROVINCIAL DE TUNGURAHUA

4.1. Plataforma tecnológica

Dentro de la planificación de la propuesta para el fortalecimiento de la red del HCPT se debe establecer el modelo jerárquico de diseño de red:

4.1.1. Capa de Núcleo

Que se encargará de transportar la información a altos niveles de velocidad entre los dispositivos de distribución y núcleo:

- Proveer de alta velocidad, baja latencia y enlaces de dispositivos para un rápido transporte de datos a través del backbone,
- Proporcionar una muy fiable y disponible backbone. Esto se logra mediante la aplicación de la redundancia en ambos dispositivos y enlaces de manera que los puntos de falla no existan, y

- Cómo adaptarse a los cambios rápidamente de red mediante la aplicación de una rápida convergencia de protocolo de enrutamiento. El protocolo de enrutamiento también puede configurarse para equilibrar la carga de más enlaces redundantes a fin de que la capacidad adicional se puede utilizar cuando no existen las fallas.

4.1.2. Capa de Distribución

En esta capa se establece:

- La aplicación de políticas de filtrado y priorización de tráfico y colas,
- Enrutamiento de acceso entre el núcleo y las capas. Si los diferentes protocolos de enrutamiento se aplican a estas otras dos capas, la capa de distribución es responsable de la redistribución (reparto) entre los protocolos de enrutamiento, filtrado y si es necesario
- Realización de ruta resumida. Cuando las rutas son resumidas, los routers sólo han resumido las rutas de sus tablas de enrutamiento, en lugar de rutas detalladas innecesarias. Esto se traduce en menores tablas de enrutamiento, lo que reduce la memoria del router requerida. Actualizaciones de enrutamiento también son más pequeños y, por tanto, utilizar menos ancho de banda en la red. La ruta resumida sólo es posible si el esquema de direccionamiento IP ha sido diseñado correctamente.

- Proporcionar las conexiones redundantes, tanto para los dispositivos de acceso y en la estructura básica de dispositivos.
- La agregación de varias conexiones de acceso de menor velocidad a mayor velocidad de las conexiones del núcleo y la conversión entre diferentes tipos de medio, si son necesarias

4.1.3. Capa de Acceso

La capa de acceso es donde los usuarios acceden a la red. Los usuarios pueden ser locales o remotos.

Los usuarios locales suelen acceder a la red a través de conexiones a un Hub o un Switch. Recordemos que los centros operan en la capa 1 OSI, y todos los dispositivos conectados a un concentrador se encuentran en la misma colisión (o ancho de banda) de dominio. Switches operan en el Nivel 2, y cada uno de los puertos en un conmutador es su propio dominio de colisiones, lo que significa que las conversaciones entre múltiples dispositivos conectados a través del conmutador pueden estar ocurriendo simultáneamente.

Los usuarios remotos pueden acceder a la red a través de Internet, utilizando conexiones VPN, por ejemplo. Conexiones a Internet puede ser a

través de dial-up, línea de abonado digital (DSL), cable, etc. Otras posibilidades incluyen el acceso WAN, como Frame Relay, líneas arrendadas, y la Red Digital de Servicios Integrados (RDSI).

La capa de acceso también debe velar porque sólo los usuarios que están autorizados a acceder a la red son admitidos.

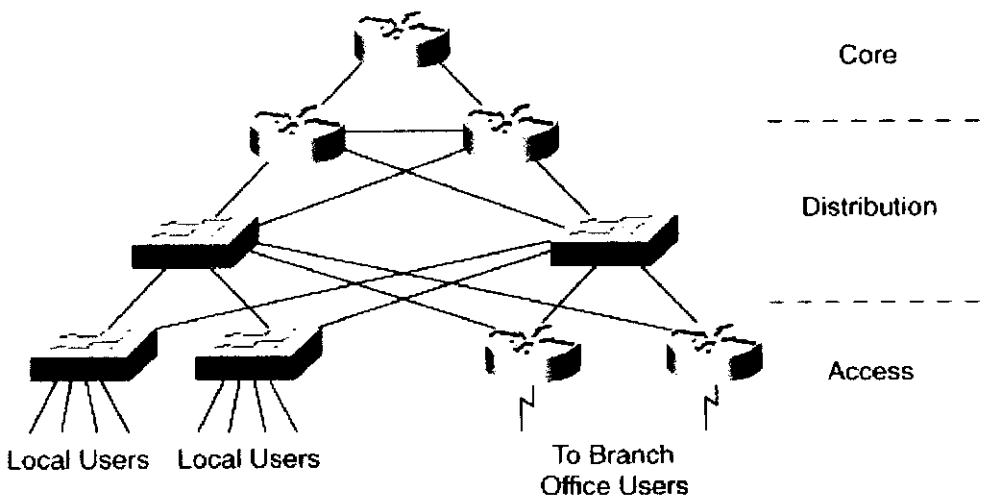


Figura 64: Modelo jerárquico[1]

De lo expuesto para nuestro caso de estudio, la **capa de núcleo** se lo debe establecer a nivel vertical de conexión entre cada piso del edificio central, utilizando para esto fibra óptica o categoría 6,

[1] **Campus Network Design Fundamentals,** porDiane Teare, Catherine Paquet, 408 páginas

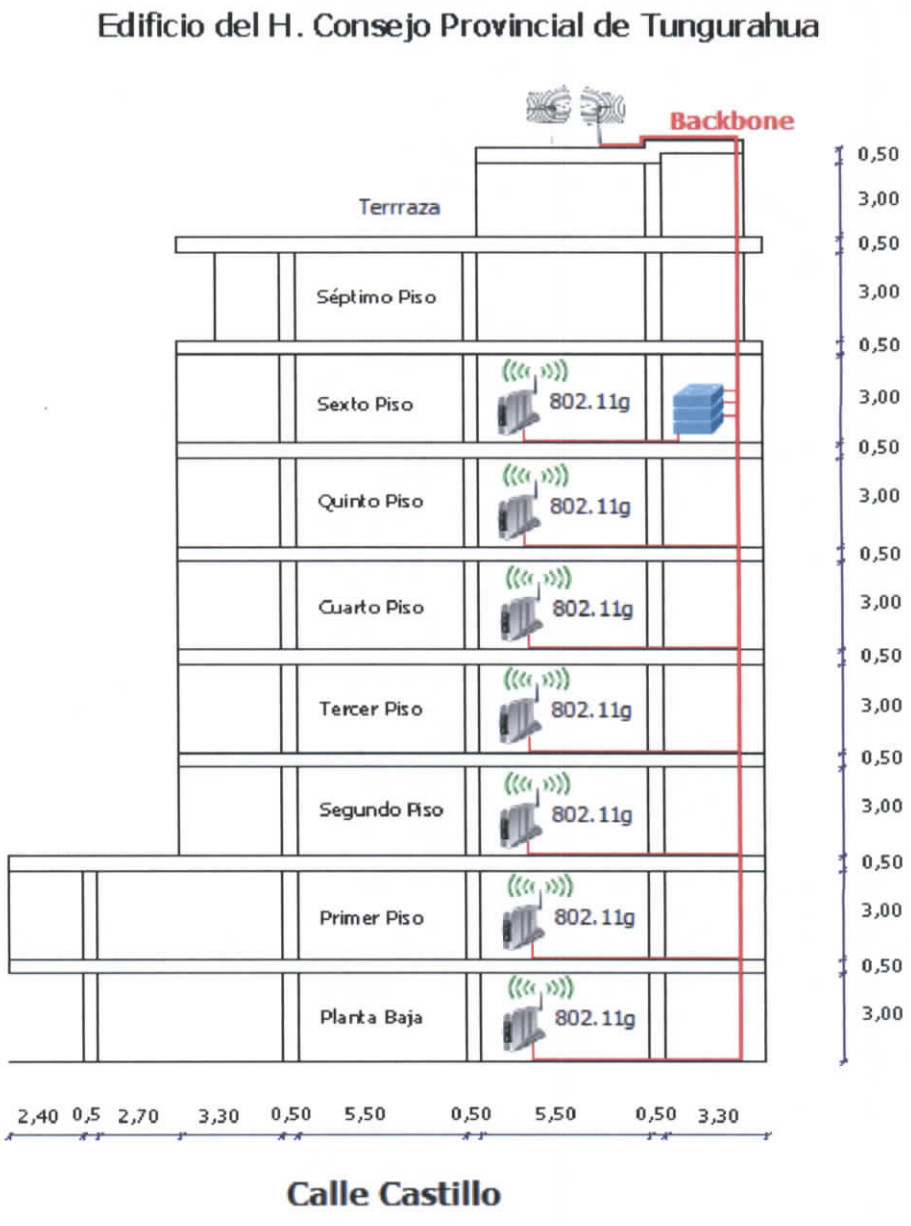


Figura 65: Backbone del Edificio Central

Pero hay que tener en consideración que actualmente la infraestructura de red es en su mayoría inalámbrica, por lo que sería un costo elevado el cambiar la tecnología actual por una nueva, en vista de que se tendría que agregar un switch capa 3 a cada piso o Departamento y ver si se elimina

cada Access Point o se conecta a este Switch, por lo que se considera la solución de incorporar un solo Switch capa 3 en el rack y el cual se comunicará a cada piso mediante cableado estructurado haciendo que este Swicth trabaje a dos capas, de núcleo y distribución.

Para este caso se utilizará el Switch Cisco Catalyst 3560G-48PS, que tiene un nivel de procesamiento interno de peticiones bien grande, además tiene 48 puertos Ethernet 10/100/1000 Mbps y 2 puertos para fibra óptica, también es un Switch capa 3 que permite hacer VLANS y ruteo entre ellas, aplicar lista de Acceso para el filtrado de peticiones.

Figura 66: Switch Catalyst 3560-48PS

Al nivel de capa de acceso se utilizarán los Access Point Orinoco que entre sus funciones principales permiten también trabajar y controlar VLANS, restricciones de acceso por MAC address, DHCP, etc.

Figura 67: Access Point Orinoco AP-4000

Para la conexión de internet se utilizará el dispositivo 3Com SuperStack 3 Switch 4226T , al cual se conectará el modem adsl, el firewall y el servidor proxy

Figura 68: 3Com SuperStack 3 Switch 4226T

Para los puntos remotos se debería cambiar o mejorar los enlaces, y pueden ser también con fibra óptica o cambiando los radios enlaces con otros equipos de comunicación que permitan tener una mejor velocidad de conexión a otra frecuencia, en vista de que en la zona donde se encuentra el edificio central se encuentran otros enlaces spread spectrum de otras empresas.

De la misma manera se procederá para el Centro de Promociones y Servicios de la Provincia, añadiendo un Switch Cisco Catalyst 3560G-48PS para administrar el tráfico y VLANs de futuras redes que se puedan crear

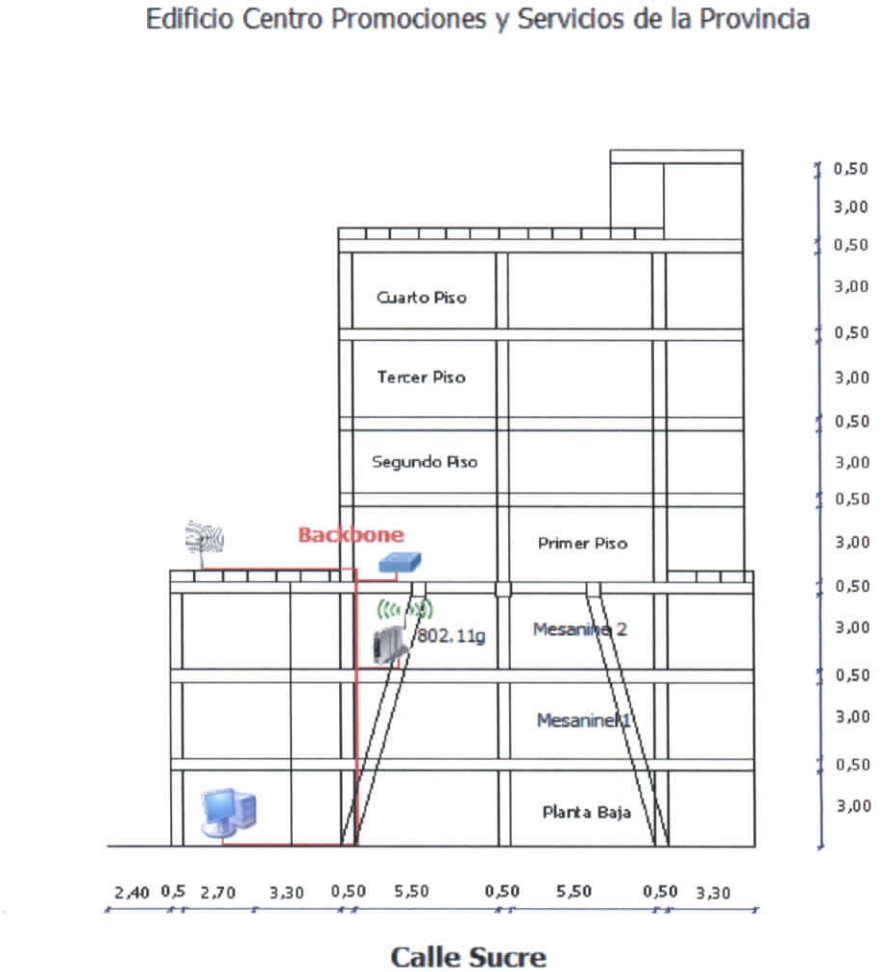


Figura 69: Backbonde del Centro de Promociones y Servicios de la Provincia

Y en vista de que en el área de bodega y talleres dispone de pocos equipos, solo se potenciarán los enlaces remotos.

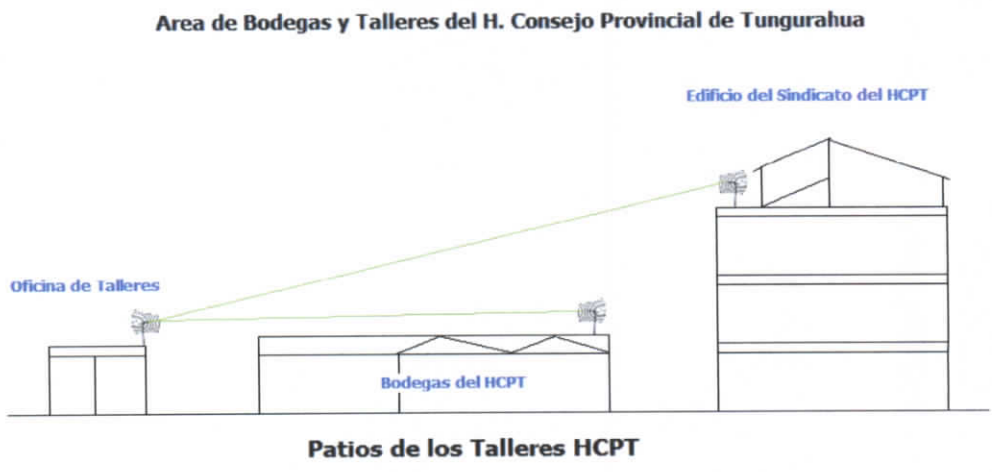


Figura 70: Area de Bodega y Talleres del HCPT

Una vez definidos los niveles de red que se utilizaran hay que definir los siguientes aspectos del diseño

4.1.4. Diseño de Switching:

Existen 168 dispositivos de red en todo el HCPT, y que en promedio máximo de cada dirección hay 16 computadores, haciendo una proyección a un incremento de recursos de red por dirección se establece el siguiente cuadro de direcciones IP para separar en dominios de broadcast y permitir la creación de VLANs, utilizando direcciones de clase B, ya que permitir utilizar más equipos a nivel corporativo y porque no son muy utilizadas como las de clase C, las cuales son utilizadas por casi todas las empresas que trabajan alrededor, y como se tienen conexión inalámbrica, se debe prevenir trabajar en el mismo grupo de direcciones IP locales

Tabla de VLANs

No.	Dirección o Departamento	# disp..	Proy.	Subnet	Mask	Rango	Broadcast
1	Administrativo	17	30	172.16.0.0	255.255.255.224	172.16.0.1 to 172.16.0.30	172.16.0.31
2	Asociación de Empleados		30	172.16.0.32	255.255.255.224	172.16.0.33 to 172.16.0.62	172.16.0.63
3	Bodega y Talleres	11	30	172.16.0.64	255.255.255.224	172.16.0.65 to 172.16.0.94	172.16.0.95
4	Desarrollo Humano y Cultura	9	30	172.16.0.96	255.255.255.224	172.16.0.97 to 172.16.0.126	172.16.0.127
5	Financiero	21	30	172.16.0.128	255.255.255.224	172.16.0.129 to 172.16.0.158	172.16.0.159
6	Gobierno Provincial, Aula Virtual, Cooperativa	27	30	172.16.0.160	255.255.255.224	172.16.0.161 to 172.16.0.190	172.16.0.191
7	Planificación y Procuraduría Síndica	12	30	172.16.0.192	255.255.255.224	172.16.0.193 to 172.16.0.222	172.16.0.223
8	Producción	13	30	172.16.0.224	255.255.255.224	172.16.0.225 to 172.16.0.254	172.16.0.255
9	Recursos Hídricos	18	30	172.16.1.0	255.255.255.224	172.16.1.1 to 172.16.1.30	172.16.1.31
10	Relaciones Externas	4	30	172.16.1.32	255.255.255.224	172.16.1.33 to 172.16.1.62	172.16.1.63
11	Sala de Consejeros	3	30	172.16.1.64	255.255.255.224	172.16.1.65 to 172.16.1.94	172.16.1.95
12	Secretaría General, Sala de Choferes	9	30	172.16.1.96	255.255.255.224	172.16.1.97 to 172.16.1.126	172.16.1.127
13	Sistemas	8	30	172.16.1.128	255.255.255.224	172.16.1.129 to 172.16.1.158	172.16.1.159
14	Vías y Construcciones	14	30	172.16.1.160	255.255.255.224	172.16.1.161 to 172.16.1.190	172.16.1.191
15	Internet	2	6	172.16.1.192	255.255.255.248	172.16.1.193 to 172.16.1.198	172.16.1.199
		168	**426**				

Tabla 36: VLANs diseñadas para el H. Consejo Provincial de Tungurahua

Para la conmutación de internet, servidor proxy y firewall configurado con las direcciones públicas 200.107.35.64/29 se utiliza el Switch 3COM 4226T, a continuación se detalla la conexión de los puertos del Switch:

Port	Dirección	Equipo	VLAN	IP	Speed	Mode	MAC
1	Internet	MT800		200.107.35.65	100 Mbps	Full Duplex	00-0F-A3-1C-04-54
12	Internet	Firewall sgs		200.107.35.68	100 Mbps	Full Duplex	00-D0-68-0D-1B-D4
24	Internet	proxy		200.107.35.66	101 Mbps	Full Duplex	00-03-BA-2A-95-72

Tabla 37: Puertos de Switch 3COM SuperStack 4226T

Y para la conmutación de distribución y núcleo se definen los puertos y VLANs que se configurarán en el Switch Catalys Cisco 3560G-48PS

Port	Dirección	Equipo	VLAN	IP	Speed	MAC
1	Internet	Firewall sgs	1	172.16.1.194	100 Mbps	00-D0-68-0D-1B-D3
2	Administrativo	HCPT_ADM_G1	10	172.16.0.2	100 Mbps	00-20-A6-5B-6F-52
3	Administrativo	AccesPoint3	10	172.16.0.3		
4	Administrativo	HP-2000 CENTRAL	10	172.16.0.6	10 Mbps	00-64-00-00-0F-11
5	Administrativo	Security	10	172.16.0.4	100 Mbps	00-0E-53-06-8F-EB
6	Administrativo	Impresora	10	172.16.0.5		08-00-37-71-2D-96
7	Asociación	Séptimo Piso	20	172.16.0.34		
8	Bodega y Talleres	extreme 2 1	30	172.16.0.66	100 Mbps	00-40-F4-B9-32-7A
9	Desarrollo Humano y Cultura	HCPT_DHC_G1	40	172.16.0.98	100 Mbps	00-20-A6-5B-25-CE
10	Financiero	SWITCH - HUB	50	172.16.0.129	100 Mbps	
11	Gobierno y Aula Virtual, Cooperativa	extreme 1 1	60	172.16.0.162	100 Mbps	00-40-F4-B8-C0-9A
12	Gobierno y Aula Virtual, Cooperativa	Cooperativa	60	172.16.0.164	100 Mbps	00-20-A6-58-3C-A2
13	Planificación y Procuraduría Síndica	HCPT_PLAN_G1	70	172.16.0.194	100 Mbps	00-20-A6-5B-69-5C
14	Producción	HCPT_PRO_G1	80	172.16.0.226	100 Mbps	00-20-A6-62-52-DB
15	Recursos Hídricos	HCPT_RRHH_G1	90	172.16.1.2	100 Mbps	00-20-A6-5B-25-DD
16	Recursos Hídricos	NPIF057F5	90	172.16.1.3	100 Mbps	00-11-0A-F0-57-F5
17	Relaciones Externas	HCPT_REX_G1	100	172.16.1.34	100 Mbps	00-20-A6-5D-68-A0
18	Sala de Consejeros	secre	110	172.16.1.65	100 Mbps	00-08-A1-31-6A-E9
19	Secretaría General	jefearchivo	120	172.16.1.100	100 Mbps	00-13-20-CC-F8-76
20	Secretaría General	prefecto	120	172.16.1.99	100 Mbps	00-07-E9-3C-D5-07

Port	Dirección	Equipo	VLAN	IP	Speed	MAC
21	Secretaría General	archivo1	120	172.16.1.101	100 Mbps	00-13-20-CC-FB-40
22	Secretaría General	AP1	120	172.16.1.102		
23	Secretaría General, Sala de Choferes	HCPT_SEC_G1	120	172.16.1.98	100 Mbps	00-20-A6-5D-68-C4
24	Sistemas	sunfv120	130	172.16.1.130	100 Mbps	00-03-BA-2A-95-72
25	Sistemas	sunfv280	130	172.16.1.131	100 Mbps	00-03-BA-23-EB-F4
26	Sistemas	mail	130	172.16.1.132	100 Mbps	00-14-4F-4C-88-75
27	Sistemas	serversystem	130	172.16.1.133	100 Mbps	00-08-A1-4A-11-1B
28	Sistemas	systems	130	172.16.1.134	100 Mbps	00-19-D1-6A-3C-77
29	Sistemas	descargas	130	172.16.1.135	100 Mbps	00-08-A1-72-80-F4
30	Vías y Construcciones	HCPT_OOPP_G1	140	172.16.1.162	100 Mbps	00-20-A6-70-7B-C5
31	Vías y Construcciones	jefefiscal	140	172.16.1.163	100 Mbps	00-19-D1-62-92-AF
32	Financiero	Yppb	50	172.16.0.144	100 Mbps	00-12-17-8A-C3-OC
33	Bodega y Talleres	Apersonal	30	172.16.0.80	100 Mbps	00-20-A6-57-EE-2B

Tabla 38: Puertos del Switch Cisco Catalyst 3560G-48PS

Entonces se establece a cada grupo, Dirección o Departamento con un número de 30 direcciones IP con proyección a que se puedan incrementar más equipos informáticos en cada departamento, por lo que se conformarían los siguientes grupos de trabajo:

VLAN Dirección Administrativa

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
DIRECCIONADM	Windows Vista	Local	TCP/IP	>172.16.0.7:5405	Administrativo
SECREADMIN	Windows XP	Local	TCP/IP	>172.16.0.9:5405	Administrativo
PERSONAL	Windows Vista	Local	TCP/IP	>172.16.0.10:5405	Administrativo
APERSONAL	Windows XP	Local	TCP/IP	>172.16.0.11:5405	Administrativo
JPERSONAL	Windows Vista	Local	TCP/IP	>172.16.0.12:5405	Administrativo
ODONTOLOGICO	Windows XP	Local	TCP/IP	>172.16.0.14:5405	Administrativo
AMARCIAL	Windows XP	Local	TCP/IP	>172.16.0.15:5405	Administrativo
HREYES	Windows XP	Local	TCP/IP	>172.16.0.16:5405	Administrativo
MEDICO1	Windows XP	Local	TCP/IP	>172.16.0.17:5405	Administrativo
ENFERMERIA	Windows XP	Local	TCP/IP	>172.16.0.20:5405	Administrativo
ELECTRICO	Windows XP	Local	TCP/IP	>172.16.0.21:5405	Administrativo
NRODRIGUEZ	Windows XP	Local	TCP/IP	>172.16.0.22:5405	Administrativo
RECAUDADOR	Windows XP	Local	TCP/IP	>172.16.0.104:5405	Administrativo

Figura 71: VLAN Administrativo

VLAN del Área de Bodega y Talleres

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
BODEGA2	Windows XP	Local	TCP/IP	>172.16.0.73:5405	Bodega
BODEGA3	Windows XP	Local	TCP/IP	>172.16.0.74:5405	Bodega
BODEGA1	Windows XP	Local	TCP/IP	>172.16.0.75:5405	Bodega

Figura 72: VLAN Bodega

VLAN de la Dirección de Desarrollo Humano y Cultura

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
PROMOTORES	Windows XP	Local	TCP/IP	>172.16.0.101:5...	Cultura
PROMOTORES2	Windows XP	Local	TCP/IP	>172.16.0.100:5...	Cultura
SECRETARIADHC	Windows XP	Local	TCP/IP	>172.16.0.102:5...	Cultura
PROMOTORES1	Windows XP	Local	TCP/IP	>172.16.0.103:5...	Cultura
DIRCULTURA	Windows XP	Local	TCP/IP	>172.16.0.99:5405	Cultura

Figura 73: VLAN Cultura

VLAN de la Dirección Financiera

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
DFPC012	Windows XP	Local	TCP/IP	>172.16.0.143:5...	Financiero
MANDRADE	Windows XP	Local	TCP/IP	>172.16.0.147:5...	Financiero
MERCYSANCHEZ	Windows XP	Local	TCP/IP	>172.16.0.135:5...	Financiero
PPYB_DIRFIN	Windows XP	Local	TCP/IP	>172.16.0.144:5...	Financiero
SERVIDORDF	Windows 2000	Local	TCP/IP	>172.16.0.132:5...	Financiero
SRICONTA3	Windows XP	Local	TCP/IP	>172.16.0.145:5...	Financiero
SUSANAVACA	Windows XP	Local	TCP/IP	>172.16.0.137:5...	Financiero
SROBAYO1	Windows XP	Local	TCP/IP	>172.16.0.140:5...	Financiero
SRICONTA1	Windows XP	Local	TCP/IP	>172.16.0.146:5...	Financiero
SACUNIA	Windows XP	Local	TCP/IP	>172.16.0.134:5...	Financiero
PATIQUINTANA	Windows XP	Local	TCP/IP	>172.16.0.136:5...	Financiero
MARTHACATU...	Windows XP	Local	TCP/IP	>172.16.0.138:5...	Financiero
ICALVACHE	Windows XP	Local	TCP/IP	>172.16.0.148:5...	Financiero
BHGB_CONTA5	Windows XP	Local	TCP/IP	>172.16.0.139:5...	Financiero

Figura 74: VLAN Financiero

VLAN del Área del Gobierno Provincial de Tungurahua

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
CIUDADANIA	Windows XP	Local	TCP/IP	>172.16.0.176:5...	Gobierno
GENTE	Windows Vista	Local	TCP/IP	>172.16.0.170:5...	Gobierno
SECREGOBIERNO	Windows Vista	Local	TCP/IP	>172.16.0.167:5...	Gobierno
TRABAJO	Windows Vista	Local	TCP/IP	>172.16.0.172:5...	Gobierno
SECTORSOCIAL	Windows Vista	Local	TCP/IP	>172.16.0.178:5...	Gobierno
PARLAMENTOS	Windows XP	Local	TCP/IP	>172.16.0.180:5...	Gobierno
GENERO	Windows XP	Local	TCP/IP	>172.16.0.175:5...	Gobierno
AGROPECUARIA	Windows XP	Local	TCP/IP	>172.16.0.174:5...	Gobierno

Figura 75: VLAN Gobierno Provincial de Tungurahua

VLAN de la Dirección de Procuraduría Síndica - Jurídico

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
ABOGACIA1	Windows Vista	Local	TCP/IP	>172.16.0.204:5...	Juridico
SECRETARIAJ	Windows XP	Local	TCP/IP	>172.16.0.202:5...	Juridico
DIRECCIONJ	Windows XP	Local	TCP/IP	>172.16.0.201:5...	Juridico
ABOGACIA	Windows XP	Local	TCP/IP	>172.16.0.203:5...	Juridico

Figura 76: VLAN Jurídico

VLAN de la Dirección de Planificación

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
GESTION	Windows XP	Local	TCP/IP	>172.16.0.200:5...	Planificacion
SECRETARIAPL...	Windows XP	Local	TCP/IP	>172.16.0.196:5...	Planificacion
PLANTEL	Windows XP	Local	TCP/IP	>172.16.0.237:5...	Planificacion
DIRPLANIFICAC...	Windows XP	Local	TCP/IP	>172.16.0.195:5...	Planificacion

Figura 77: VLAN Planificación

VLAN de la Dirección de Producción

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
DIRPRODUCCI...	Windows XP	Local	TCP/IP	>172.16.0.198:5...	Produccion
MMORA	Windows XP	Local	TCP/IP	>172.16.0.231:5...	Produccion
SECRETARIAPR...	Windows XP	Local	TCP/IP	>172.16.0.199:5...	Produccion
VETERINARIO	Windows XP	Local	TCP/IP	>172.16.0.239:5...	Produccion
TURISMO	Windows XP	Local	TCP/IP	>172.16.0.232:5...	Produccion
PIRT	Windows XP	Local	TCP/IP	>172.16.0.228:5...	Produccion
EMPRESAVIAL	Windows XP	Local	TCP/IP	>172.16.0.227:5...	Produccion
DESARROLLO2	Windows XP	Local	TCP/IP	>172.16.0.230:5...	Produccion

Figura 78: VLAN Producción

VLAN de la Dirección de Recursos Hídricos y Saneamiento Ambiental

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
ASISTENTERRHH	Windows XP	Local	TCP/IP	>172.16.1.20:5405	Recursos Hidricos
DIRECCIONRRHH	Windows XP	Local	TCP/IP	>172.16.1.4:5405	Recursos Hidricos
DISENIORRHH	Windows XP	Local	TCP/IP	>172.16.1.6:5405	Recursos Hidricos
FISCAL3RRHH	Windows XP	Local	TCP/IP	>172.16.1.15:5405	Recursos Hidricos
JFISCAL	Windows XP	Local	TCP/IP	>172.16.1.9:5405	Recursos Hidricos
PASANTEAMBI...	Windows XP	Local	TCP/IP	>172.16.1.21:5405	Recursos Hidricos
TOPORRHH	Windows XP	Local	TCP/IP	>172.16.1.13:5405	Recursos Hidricos
SECRETARIARR...	Windows XP	Local	TCP/IP	>172.16.1.5:5405	Recursos Hidricos
JMEDIOAMBIE...	Windows XP	Local	TCP/IP	>172.16.1.16:5405	Recursos Hidricos
GAMBIENTAL1	Windows XP	Local	TCP/IP	>172.16.1.17:5405	Recursos Hidricos
FISCAL2RRHH	Windows XP	Local	TCP/IP	>172.16.1.12:5405	Recursos Hidricos
DISENIODIAGR...	Windows XP	Local	TCP/IP	>172.16.1.8:5405	Recursos Hidricos
COMPUTORRHH	Windows XP	Local	TCP/IP	>172.16.1.14:5405	Recursos Hidricos
AMBIENTE	Windows XP	Local	TCP/IP	>172.16.1.18:5405	Recursos Hidricos

Figura 79: VLAN Recursos Hídricos

VLAN de la Dirección de Relaciones Externas

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
DIRRELAEXTER...	Windows XP	Local	TCP/IP	>172.16.1.35:5405	Relaciones Externas
SECRERREE	Windows XP	Local	TCP/IP	>172.16.1.107:5...	Relaciones Externas
PRENSA	Windows XP	Local	TCP/IP	>172.16.1.106:5...	Relaciones Externas
COE	Windows XP	Local	TCP/IP	>172.16.1.36:5405	Relaciones Externas

Figura 80: VLAN Relaciones Externas

VLAN de la Dirección de Secretaría General

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
JEFEARCHIVO	Windows XP	Local	TCP/IP	>172.16.1.100:5...	Secretaría General
PREFECTO	Windows XP	Local	TCP/IP	>172.16.1.99:5405	Secretaría General
SECPREFECTURA	Windows XP	Local	TCP/IP	>172.16.1.103:5...	Secretaría General
SECGENERAL	Windows XP	Local	TCP/IP	>172.16.1.104:5...	Secretaría General
NANCY	Windows XP	Local	TCP/IP	>172.16.1.105:5...	Secretaría General
ARCHIVO1	Windows XP	Local	TCP/IP	>172.16.1.101:5...	Secretaría General

Figura 81: VLAN Secretaría General

VLAN de la Unidad de Sistemas

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
DESCARGAS	Windows XP	Local	TCP/IP	>172.16.1.135:5...	Sistemas
SERVERHCPT	Windows 2003	Local	TCP/IP	>172.16.1.133:5...	Sistemas
proxy	SuSE	Local	TCP/IP	>172.16.1.130:5...	Sistemas
DATABASE	Windows XP	Local	TCP/IP	>172.16.0.8:5405	Sistemas

Figura 82: VLAN Sistemas

VLAN de la Dirección Vías y Construcciones – Obras Públicas

Nombre	Plataforma Cliente	Estado	Trans...	Dirección	Ubicación
DIRECCIONOOPP	Windows XP	Local	TCP/IP	>172.16.1.165:5...	Vias y Construcci...
FISCAL2OOPP	Windows XP	Local	TCP/IP	>172.16.1.173:5...	Vias y Construcci...
GISOOPP	Windows XP	Local	TCP/IP	>172.16.1.174:5...	Vias y Construcci...
JEFEVIAS	Windows XP	Local	TCP/IP	>172.16.1.172:5...	Vias y Construcci...
TALLERES	Windows XP	Local	TCP/IP	>172.16.0.76:5405	Vias y Construcci...
UFVT1	Windows XP	Local	TCP/IP	>172.16.1.175:5...	Vias y Construcci...
VIASOOPP	Windows XP	Local	TCP/IP	>172.16.1.171:5...	Vias y Construcci...
UFVT2	Windows XP	Local	TCP/IP	>172.16.1.176:5...	Vias y Construcci...
TOPOGRAFOOPP	Windows XP	Local	TCP/IP	>172.16.1.167:5...	Vias y Construcci...
SECREOOPP	Windows XP	Local	TCP/IP	>172.16.1.166:5...	Vias y Construcci...
JEFEFISCAL	Windows XP	Local	TCP/IP	>172.16.1.163:5...	Vias y Construcci...
FISCALOOPP	Windows XP	Local	TCP/IP	>172.16.1.169:5...	Vias y Construcci...
DISENIOOPP	Windows XP	Local	TCP/IP	>172.16.1.168:5...	Vias y Construcci...
CONSTRUOOPP	Windows XP	Local	TCP/IP	>172.16.1.170:5...	Vias y Construcci...

Figura 83 VLAN Vías y Construcciones

4.1.5. Diseño de Ruteo

Para el ruteo de cada VLAN se utilizará el protocolo de ruteo RIP versión 2 que permite CIDR y que facilita agrupar bloques de direcciones IP, y además el protocolo converge cada 30 segundos y la distancia administrativa es 120, por lo tanto hay que definir las rutas que se utilizara en el diseño de red

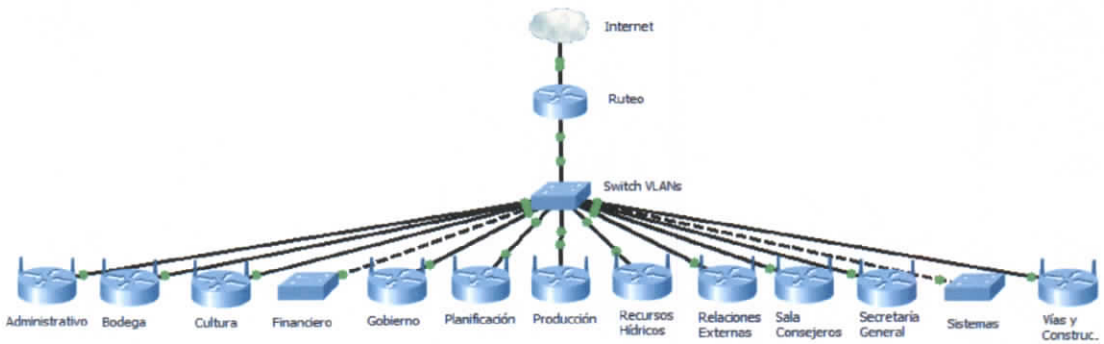


Figura 84: Esquema de rutas del HCPT

Definición de la dirección de la ruta resumida para el ruteo

Ruta	IP	DIRECCION IP				Máscara	Máscara				/
		1er Octeto	2do Octeto	3er Octeto	4to Octeto		1er Octeto	2do Octeto	3er Octeto	4to Octeto	
Administrativo	172.16.0.0	101001100	00010000	00000000	00000000	255.255.255.224	11111111	11111111	11111111	11100000	27
Asociacion	172.16.0.32	101001100	00010000	00000000	00100000	255.255.255.224	11111111	11111111	11111111	11100000	27
Bodega y Talleres	172.16.0.64	101001100	00010000	00000000	01000000	255.255.255.224	11111111	11111111	11111111	11100000	27
Desarrollo Humano y Cultura	172.16.0.96	101001100	00010000	00000000	01100000	255.255.255.224	11111111	11111111	11111111	11100000	27
Financiero	172.16.0.128	101001100	00010000	00000000	10000000	255.255.255.224	11111111	11111111	11111111	11100000	27
Gobierno Provincial, Aula Virtual, Cooperativa	172.16.0.160	101001100	00010000	00000000	10100000	255.255.255.224	11111111	11111111	11111111	11100000	27
Planificación y Procuraduría Síndica	172.16.0.192	101001100	00010000	00000000	11000000	255.255.255.224	11111111	11111111	11111111	11100000	27
Producción	172.16.0.224	101001100	00010000	00000000	11100000	255.255.255.224	11111111	11111111	11111111	11100000	27
Recursos Hídricos	172.16.1.0	101001100	00010000	00000001	00000000	255.255.255.224	11111111	11111111	11111111	11100000	27
Relaciones Externas	172.16.1.32	101001100	00010000	00000001	00100000	255.255.255.224	11111111	11111111	11111111	11100000	27
Sala de Consejeros	172.16.1.64	101001100	00010000	00000001	01000000	255.255.255.224	11111111	11111111	11111111	11100000	27
Secretaría General, Sala de Choferes	172.16.1.96	101001100	00010000	00000001	01100000	255.255.255.224	11111111	11111111	11111111	11100000	27
Sistemas	172.16.1.128	101001100	00010000	00000001	10000000	255.255.255.224	11111111	11111111	11111111	11100000	27
Vías y Construcciones	172.16.1.160	101001100	00010000	00000001	10100000	255.255.255.224	11111111	11111111	11111111	11100000	27
Internet	172.16.1.192	101001100	00010000	00000001	11000000	255.255.255.248	11111111	11111111	11111111	11111000	29
Sumarización	IP	**101001100**	**00010000**	**0000000X**	**XXXXXXXX**		11111111	11111111	11111110	00000000	
		172	**16**	**0**	**0**		**255**	**255**	**254**	**0**	
CIDR – Ruta resumida	**172.16.0.0**					**255.255.254.0**					**23**

Tabla 39: Tabla de rutas del HCPT y CIDR

Por lo tanto la dirección de red que se configurará en el Switch Cisco 3560G-PS con el protocolo de ruteo RIP versión 2 será: 172.16.0.0/23

4.1.6. Diseño de La red Inalámbrica

Actualmente el servicio de red inalámbrica ya existe en el HCPT por lo que solo se deberán establecer las seguridades necesarias para impedir el acceso no autorizado de otros usuarios a la red.

- **Desactivar SSID Broadcast.** Siendo uno de los datos necesarios para poder conectar nuestra red, es importante no divulgarlo de manera tan evidente.
- **Filtrado de direcciones MAC.** Al activar el filtrado de direcciones MAC del dispositivo inalámbrico estamos autorizando el acceso al mismo únicamente a las tarjetas de red que introduzcamos en la lista.
- **WEP (Wired Equivalent Privacy) o Privacidad Equivalente a Cableado**. Nos ofrece dos niveles de seguridad, encriptación a 64 o 128 bit. La encriptación usa un sistema de claves. La clave del ordenador debe coincidir con la clave del dispositivo inalámbrico.
- **WPA (Wireless Protected Access).** Ofrece dos tipos de seguridad, con servidor de seguridad y sin servidor. Este método se basa en tener una clave compartida de un mínimo de 8 caracteres alfanuméricos para todos los puestos de la red (Sin servidor) o disponer de un cambio dinámico de claves entre estos puestos (Con servidor). Es una opción más segura, pero no todos los dispositivos inalámbricos lo soportan.

- **RADIUS** es un protocolo de red que utiliza los servidores de acceso para proporcionar una gestión centralizada de acceso a las grandes redes, entre estas soluciones podemos mencionar por ejemplo a FreeRadius.

A continuación se muestran los esquemas de cómo se deberían conectar los dispositivos inalámbricos de red con las VLANs definidas anteriormente.

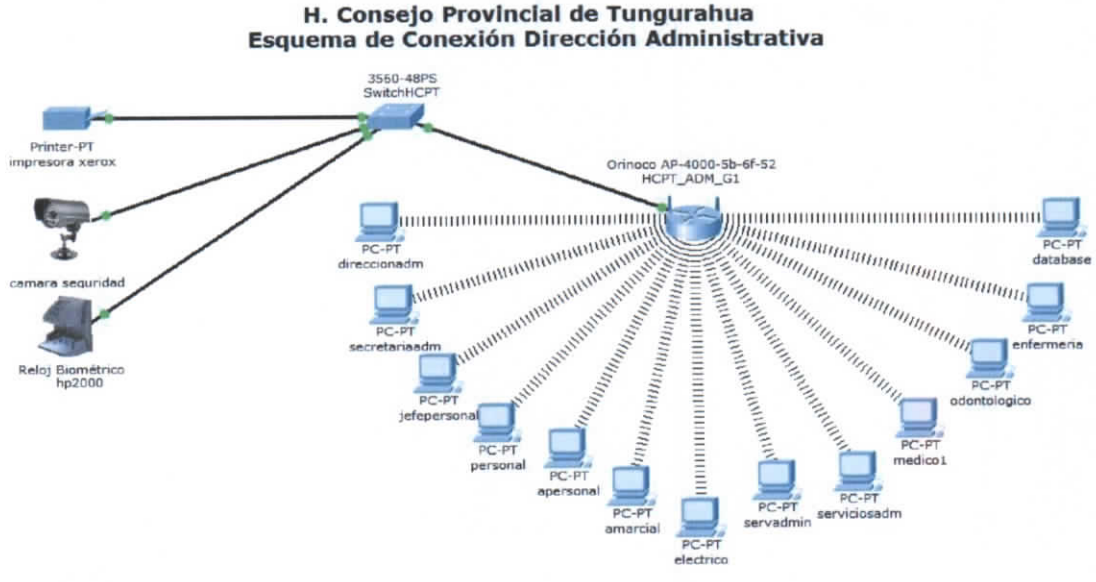


Figura 85: Wireless Administrativo

H. Consejo Provincial de Tungurahua
Esquema de Conexión Área de Bodega y Talleres

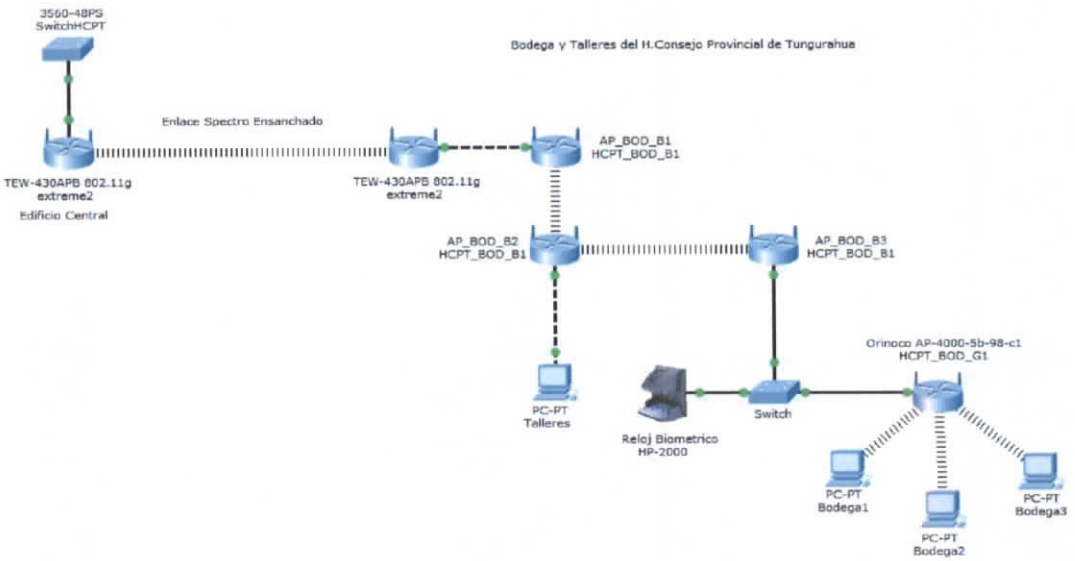


Figura 86: Wireless Bodega y Talleres

H. Consejo Provincial de Tungurahua
Esquema de Conexión Dirección Desarrollo Humano y Cultura

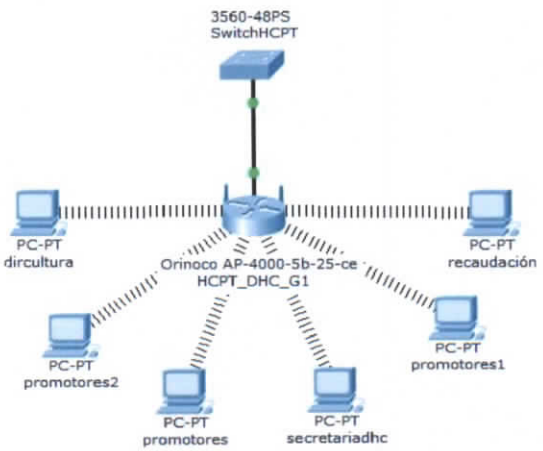


Figura 87: Wireless Cultura

H. Consejo Provincial de Tungurahua
Esquema de Conexión Dirección Financiera

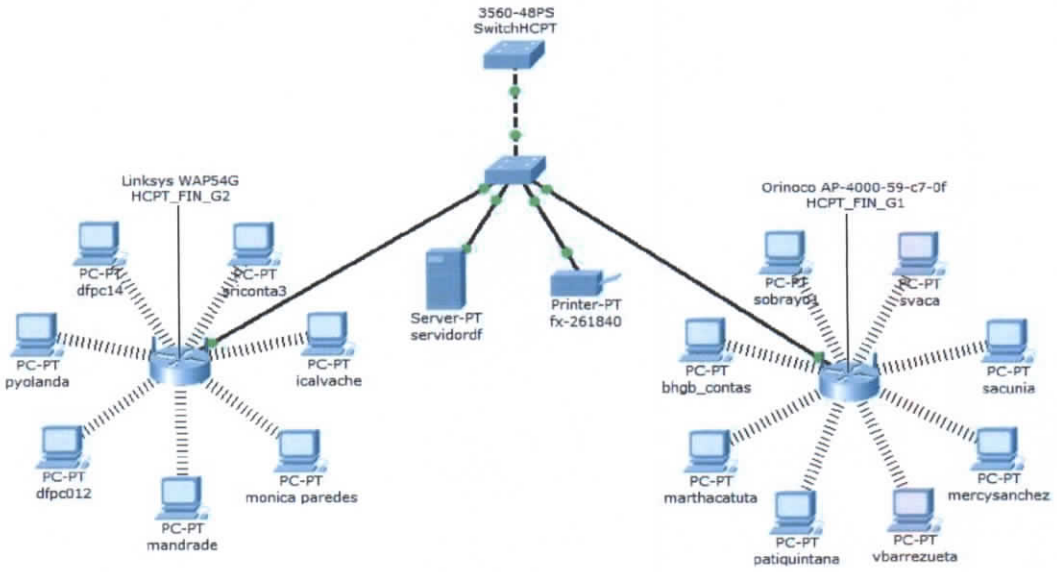


Figura 88: Wireless Financiero

H. Consejo Provincial de Tungurahua
Esquema de Conexión Gobierno Provincial

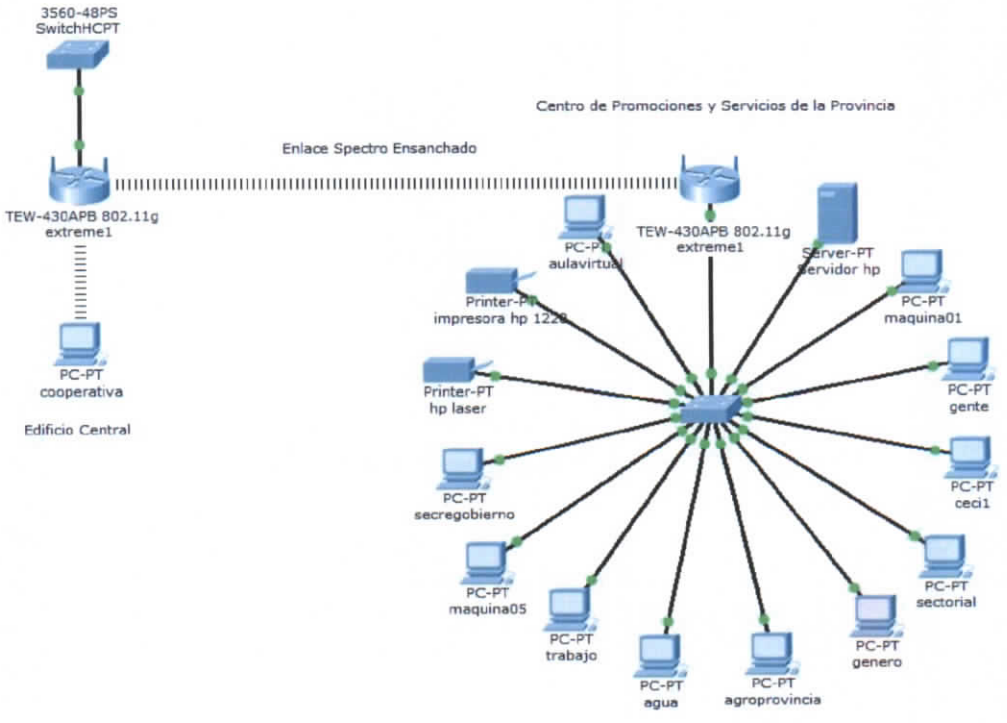


Figura 89 : Conexión a Gobierno Provincial de Tungurahua

H. Consejo Provincial de Tungurahua
Esquema de Conexión Dirección Planificación - Jurídico

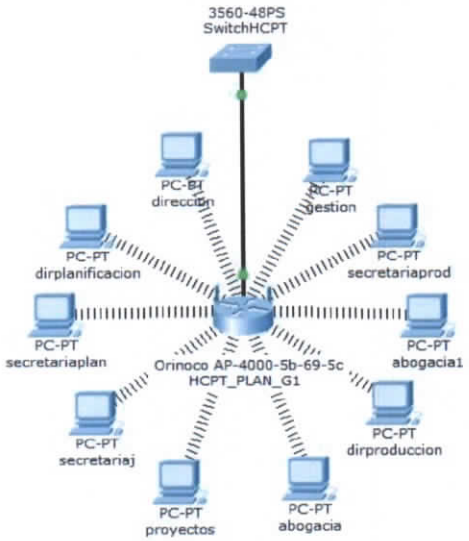


Figura 90: Wireless Planificación y Jurídico

H. Consejo Provincial de Tungurahua
Esquema de Conexión Dirección de Producción

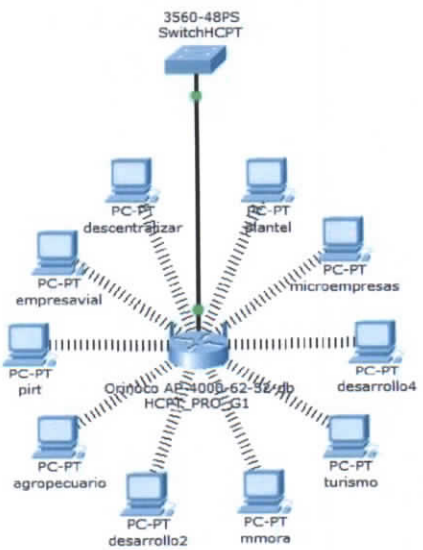


Figura 91: Wireless Producción

H. Consejo Provincial de Tungurahua
Esquema de Conexión Dirección Recursos Hídiricos

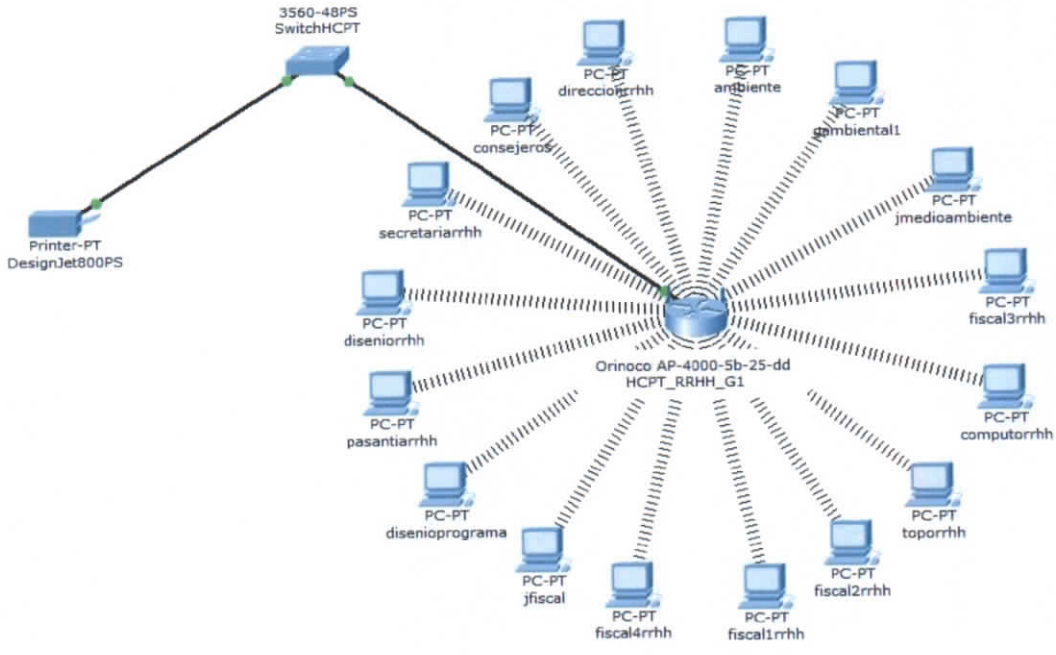


Figura 92: Wireless Recursos Hídricos

H. Consejo Provincial de Tungurahua
Esquema de Conexión Dirección Relaciones Externas

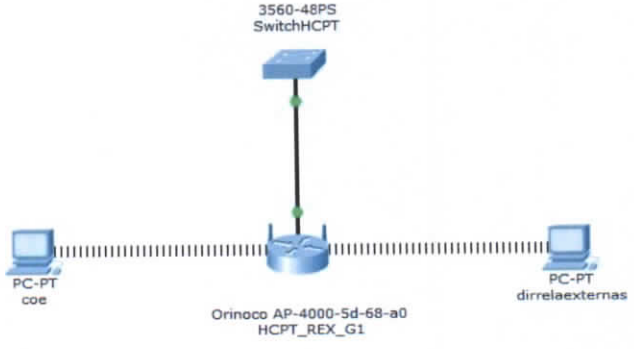


Figura 93: Wireless Relaciones Externas

H. Consejo Provincial de Tungurahua
Esquema de Conexión Dirección Secretaría General

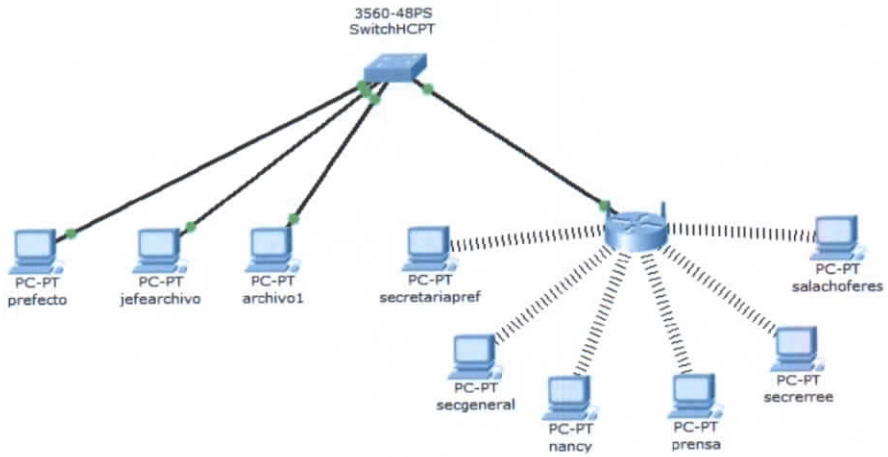


Figura 94: Wireless Secretaría General

H. Consejo Provincial de Tungurahua
Esquema de Conexión Área de Sistemas Informáticos

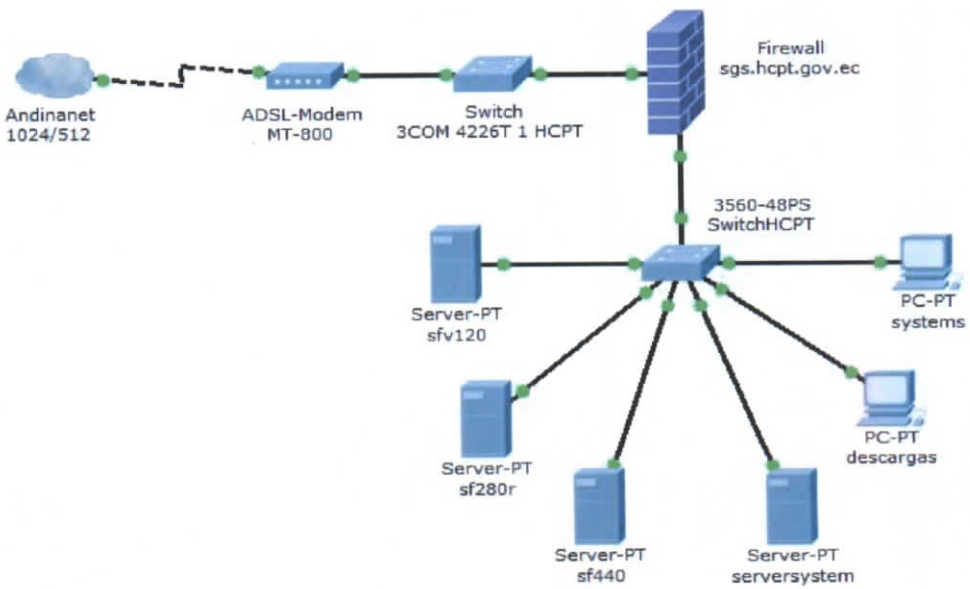


Figura 95: Conexión de la unidad de Sistemas

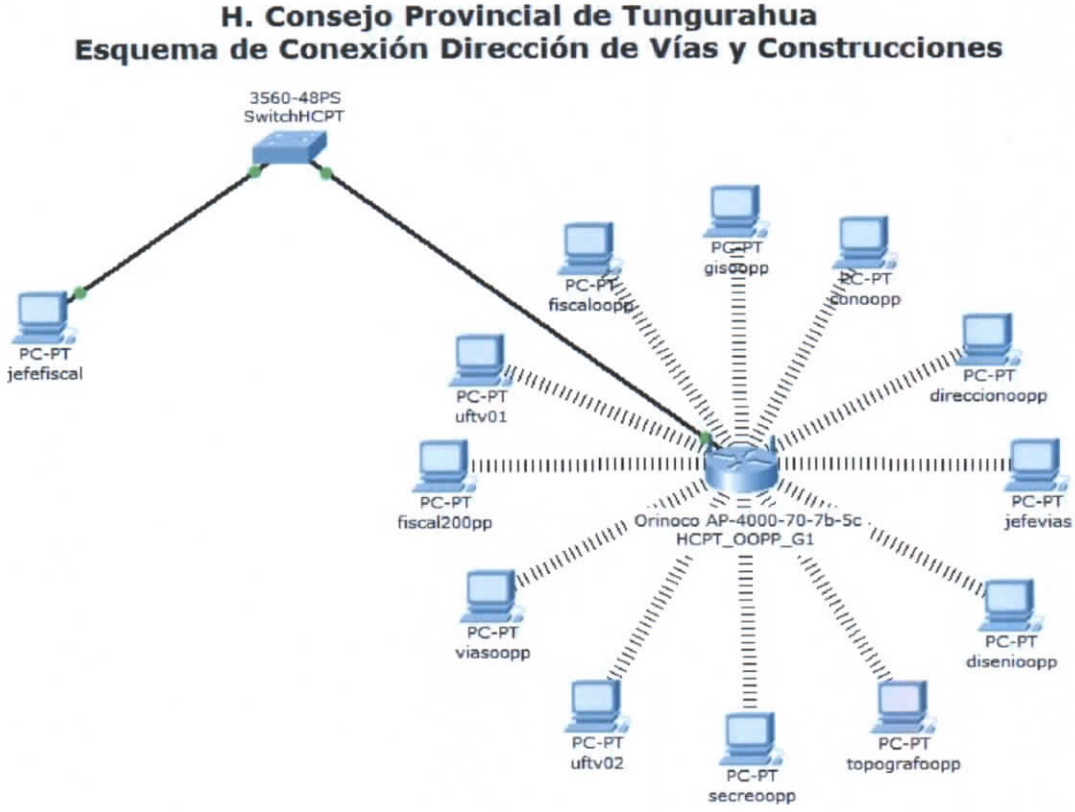


Figura 96: Wireless Vías y Construcciones

Por lo que dentro de las seguridades que se proponen, se sugiere crear una lista de acceso o reglas para el acceso a los recursos, en las cuales pueden ser agrupados por VLANs, y así dar prioridad a los grupos que manejan información critica como el Departamento Financiero, Administrativo, Base de Datos, Prefectura y el archivo de Secretaría General.

A continuación se ilustra una propuesta de las reglas que se incluirían en el Firewall

Reglas para los recursos de red por VLANS

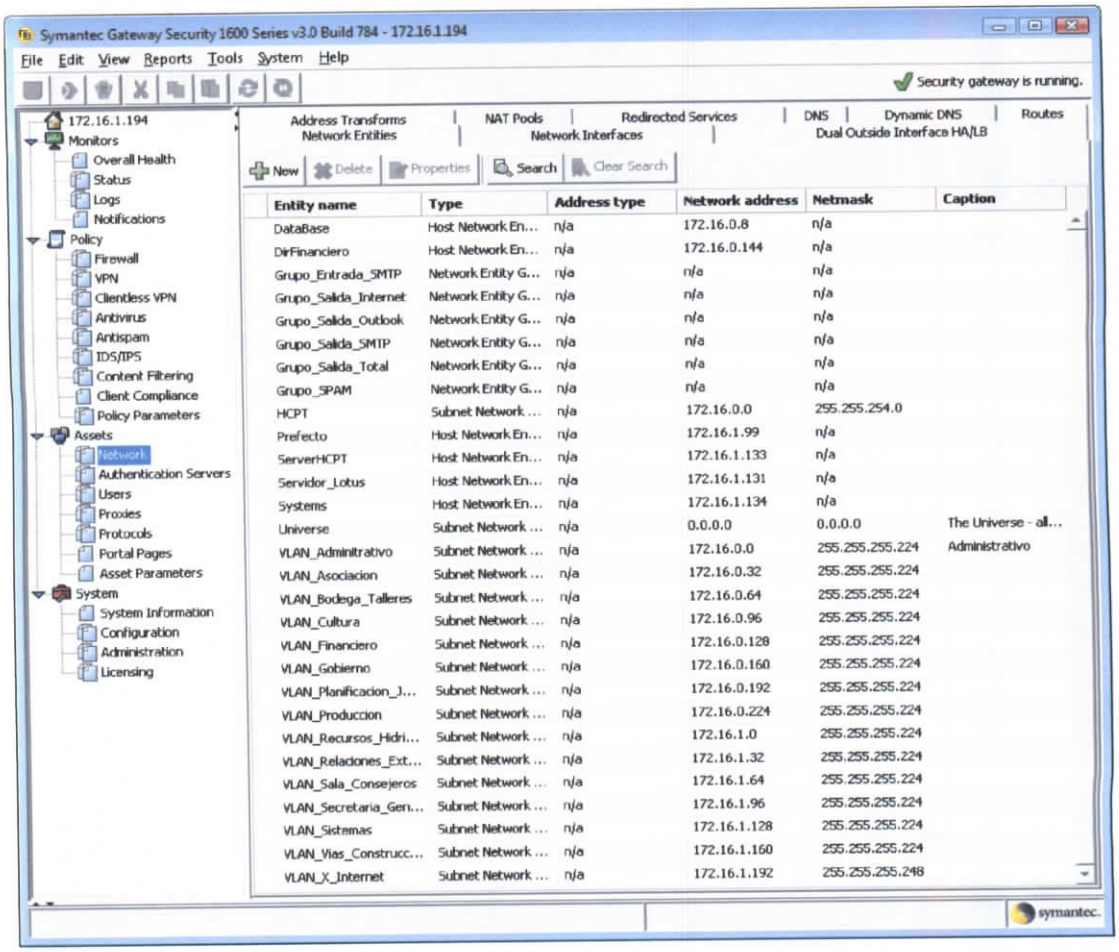


Figura 97: Symantec Gateway Security 1600 Series - Identificadores de red

4.2. Establecer los servicios informáticos institucionales

Los servicios que se indican en el capítulo 2, son los mismos que se utilizarán aquí y se los divide en dos grupos: los servicios de red, necesarios para la conexión a red, internet, seguridades, correo electrónico, y las aplicaciones para el desarrollo de las actividades y procesos de compras, control de personal, contabilidad.

También se identificaron las aplicaciones que se desea optimizar para proporcionar más servicios al manejo de documentación y procesos, como por ejemplo Administración de trámites, control de combustibles, control de bienes, control de soporte y mantenimiento de equipos, mapas virtuales, presupuestos y precios unitarios, Control de avance de obras, etc.

Servicios de red

Servicio	Servidor	Plataforma Servidor	Plataforma Clientes
Firewall	Symantec Gateway Security	Linux	
Internet Compartido	Squid 2.78	Solaris 9	Windows 98, Me,2000, XP, Vista
Internet Compartido Provisional	Squid 2.78	Suse 10.3	Windows 98, Me,2000, XP, Vista
Correo electrónico	Lotus Domino 7.01	Solaris 9	Windows 98, Me,2000, XP, Vista, Lotus Notes8
Antivirus	Symantec EndPoint Protection 11	Windows 2003 Enterprise	Windows 98, Me,2000, XP, Vista
Controlador de Dominio	Active Directory	Windows 2003 Enterprise	Windows 98, Me,2000, XP, Vista
DNS	DNS Server	Windows 2003 Enterprise	Windows 98, Me,2000, XP, Vista

Tabla 40: Servicios de Red

Servicios de Aplicaciones

Servicio	Servidor	Plataforma Servidor	Plataforma Clientes
Adquisición de Materiales	base datos documentales de Lotus Domino	Solaris 9	Windows 98, Me,2000, XP, Vista, Lotus Notes 8
Sistema de Control de Recursos Humanos	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	Windows 98, Me,2000, XP, Vista, Clientes de la aplicación y Oracle
Sistema Médico Odontológico	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	Windows 98, Me,2000, XP, Vista, Clientes de la aplicación y Oracle
Sistema de Control de Proveedores	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10	Windows 98, Me,2000, XP, Vista, Clientes de la aplicación y Oracle
Sistema Financiero FINANSG	Aplicación en Visual FOX 6 con base de datos de SQL 200 Server	Windows 2000 Advanced Server	Windows 98, Me,2000, XP, Vista, Cliente de la aplicación

Tabla 41: Servicios de aplicaciones

Servicios a Implementar

Servicio	Servidor	Plataforma Servidor
RADIUS para Autenticación de MAC Address	FreeRADIUS	Solaris 10
Protocolo de la Configuración de Host Dinámico, asignación automáticas de IP	DHCP Server sobre y dispositivos de comunicación inalámbricos	Windows 2003 server Enterprise
Sistema de Administración de Trámites y Solicitudes	Lotus Domino 7.01	Solaris 9
Sistema de Control de Combustibles	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10
Sistema de Control de bienes e inventario	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10
Sistema de Administración y Control de Soporte y Mantenimiento de Equipos	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10
Sistema de Administración y Control de Contratos y Obras	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10
Sistema de Precios Unitarios y Presupuestos	Aplicación en Visual Studio con base datos de Oracle 10g	Solaris 10
Sistema de Mapas Virtuales	Aplicación en Java con base datos de Oracle 10g	Solaris 9

Tabla 42: Servicios a Implementar

A esto hay que sumar los servicios que a futuro cercano puedan ofrecerse y dejar un soporte en la tecnología para compensar la proyección a la innovación de la tecnología, como el caso de las VozIP.

4.3. Calidad de Servicio

Debido a que el Switch Catalys Cisco 3560G-48PS tiene incorporado dentro del sistema operativo las características de manejo de QoS, se puede habilitar este servicio a nivel de la capa de distribución para que ayude en el manejo del tráfico de red y priorice los servicios para datos, voz y video, por lo que clasificaremos el tráfico según las aplicaciones con las que trabajan el

HCPT y estableceremos un porcentaje del ancho de banda para un servicio óptimo, utilizando para esto una de las herramientas de Calidad de Servicio de Cisco que se basa en los lineamientos básicos de las directrices clasificación y Marcado de Tráfico empresarial.

Clasificación del Tráfico de Red

Prioridad	Clase de Modelo	Aplicación	Valor IPP	Descripción del tráfico	% Ancho Banda
11	Tiempo real	Ruteo IP	6	Para los protocolos de ruteo y comunicación de los datos	10,00
10		Voz	5	Para voz sobre IP	20,00
9		Video Interactivo	4	Para video conferencias	20,00
8		Video continuo	4	para transmitir videos en línea	
7	Datos Críticos	Datos de misión critica	3	Tráfico de transacciones financieras o video conferencias	15,00
6		Señalización de llamadas	3	Para la inicialización de llamadas	
5		Datos transaccionales	2	Tráfico de transacciones de aplicaciones de base de datos como Recursos Humanos, Lotus domino, Oracle, etc. Para la navegación de computadores importantes	15,00
4		Administración de red	2	Para programas y protocolos de administración de la red	
3		Volumen de datos	1	Operación de sincronización y replicación de base de datos	10,00
2	Mejor esfuerzo	Minería de datos	1	Para procesos de búsqueda intensa de herramientas complejas	
1	Minería de datos	Mejor esfuerzo	0	Operación de sincronización y replicación de base de datos	10,00

Tabla 43: Clasificación del Tráfico de Red del HCPT.

4.4. Codificación y Nomenclatura de dispositivos de red

Para describir una nomenclatura que ayude a identificar los dispositivos de red se utilizarán los siguientes factores:

Factor	Caracteres del código
Infraestructura Física	2
Direcciones o Departamentos	2
Ubicación	2
Tipo de Dispositivo	2
Acceso al Medio	2
Cantidad de dispositivos	3
Total	**13**

Tabla 44: Tabla de factores para la Normalización

Dentro de las Infraestructuras físicas del consejo utilizaremos los siguientes códigos

Código	descripción
EC	Edificio Central
PS	Centro de Promociones y Servicios
BT	Bodega y Talleres
PF	Parque de la Familia
PI	Granja de Píllaro
CA	Vivero Catiglata

Tabla 45: Tabla de codificación de las infraestructuras físicas del HCPT

Para Direcciones o Departamento se utilizarán los siguientes códigos

Código	descripción
CU	Desarrollo Humano y Cultura
SG	Secretaría General
RE	Relaciones Externas
FN	Financiero
RH	Recursos Hídricos
SC	Sala de Consejeros
VC	Vías y Construcciones
PL	Planificación
JU	Procuraduría Síndica - Jurídico

Código	descripción
PR	Producción
AD	Administrativo
SY	Sistemas
AE	Asociación de Empleados
CO	Cooperativa
AV	Aula Virtual
BM	Biblioteca del Municipio
BC	Biblioteca del HCPT
GP	Gobierno Provincial
TA	Talleres
BO	Bodega
SN	Sindicato

Tabla 46: Codificación de las Direcciones y departamentos del HCPT

Para las ubicaciones los siguientes códigos

Código	Descripción
PB	Planta Baja
P1	Piso 1
P2	Piso 2
P3	Piso 3
P4	Piso 4
P5	Piso 5
P6	Piso 6
P7	Piso 7
TC	Terraza HCPT
M1	Mezzanine 1
M2	Mezzanine 2
TG	Terraza Gobierno Provincial
TS	Terraza Sindicato

Tabla 47: Codificación de Ubicaciones del HCPT

Para los tipos de dispositivos serán los siguientes códigos

Código	Descripción
SV	Servidores
PC	Computador
FW	Firewall
SW	Switch
AP	Access Point

Código	Descripción
SP	Spread Spectrum
IM	Impresora
RB	Reloj Biométrico
MD	Modem
LP	Laptop
SG	Equipos de Seguridad
OT	Otros

Tabla 48: Codificación por tipos de dispositivos

Para los tipos de acceso a la red se tendrán los siguientes códigos

Código	Descripción
FO	Fibra óptica
WL	Wireless – Inalambrica
CB	Conexión Con Cable
NC	No conectado

Tabla 49: Codificación por tipo de acceso

Y la cantidad de dispositivos se lo hará de forma secuencial con tres dígitos por los que se puede alcanzar cantidades desde 001 hasta 999 dispositivos.

Este código será único para cada Equipo y tendrá un total de 13 dígitos, y permitirá tener una mejor administración de los recursos

Ejemplo de la codificación: Se tiene un Switch que pertenece al Departamento de Sistemas y está ubicado en el sexto piso del edificio

central del HCPT, se conecta mediante cable de red y es el primer Switch tendrá el siguiente código para este equipo.

Edificio Central = EC

Sistemas = SY

Sexto Piso = P6

Switch = SW

Conexión con cable= CB

Primer dispositivo = 001

Por lo que el código de identificación será = **ECSYP6SWCB001**

Y este código también puede ser utilizado como nombre de host del dispositivo de red, o como campo clave para los registros de inventario del departamento de bienes y activos fijos.

Otro ejemplo de la codificación: Tenemos un Computador que pertenece al Gobierno Provincial y está ubicado en el primer piso del edificio de centro de Promociones y Servicios de la provincia del Tungurahua, el cual se conecta

inalámbricamente a la red y es el tercer computador, por lo que tendrá el siguiente código para este equipo.

Promociones y Servicios = PS

Gobierno Provincial = GP

Primer Piso = P1

Computador = PC

Conexión inalámbrica = WL

Tercer dispositivo = 003

Por lo que el código de identificación será = **PSGPP1PCWL003**

Cabe señalar que esta nomenclatura tendrá continuamente que seguir codificando, si aparecen nuevos dispositivos, otras maneras de conexión, si se crean otros departamentos, o si se adquieren o construyen otras infraestructuras físicas, etc.

4.5. Políticas informáticas institucionales

Definimos las líneas generales o básicas que la institución debería controlar para un buen uso de la tecnología, estas deben ser establecidas por el

Departamento de Tecnología de la Información y Comunicación, conjuntamente con un Comité de Seguridad Informática y la Dirección Administración General del HCPT o en coordinación de la Prefectura

En vista de que no existe el Departamento de Tecnología de la Información y Comunicación (TIC's), primeramente se debería crear o a su vez potenciar a la Unidad existente; a continuación se presenta una propuesta de cómo debería conformarse este departamento deTIC's, con las áreas de alcance de tecnología y las actividades que realizarían.

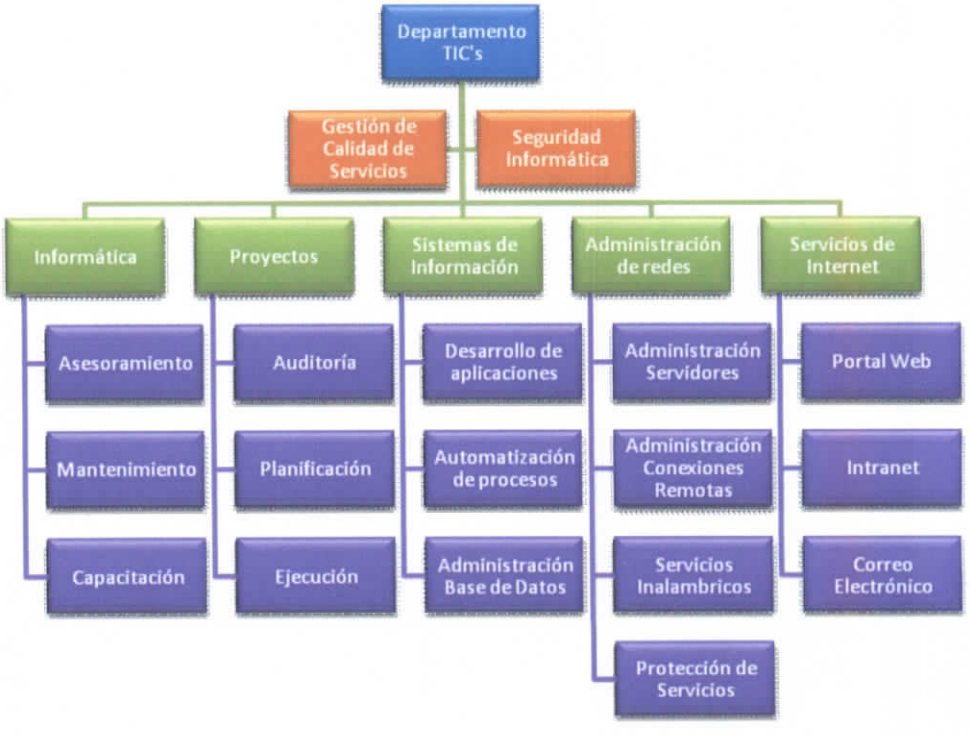


Figura 98: Organigrama Funcional del Departamento de TIC's

El Departamento de TIC's del HCPT estará conformada por cinco áreas de servicio, Los servicios son Informática, Proyectos, Sistemas de Información. Redes y Servicios de Internet, y, éstos se encargarán de brindar servicio directo al usuario, por el ámbito de competencia que tiene cada uno de ellos en materia de informática, desde el equipamiento, instalación, alteración, cambio de lugar, programación, mantenimiento, protección, etc.

De esta manera habría una mejor administración y control de las políticas de Seguridad Informáticas, las cuales tendrían su campo de acción sobre los siguientes lineamientos:

- Seguridad Física y del Ambiente
- Seguridad de las Comunicaciones y de las Operaciones
- Seguridad del Personal de TICs
- Control de Accesos
- Desarrollo e Implementación de Sistemas
- Continuidad del Negocio (desarrollo de tecnologías informáticas para los servicios que ofrece la Institución)
- Capacitación al personal

De esta manera se emite una propuesta de políticas de seguridades para la Red informática del HCPT (Red-HCPT), que es el nombre oficial de un conjunto de recursos y facilidades informáticas, de la infraestructura de telecomunicaciones y servicios asociados a ellos, provistos por el

Departamento de TIC's, pero para esto hay que definir normas y procedimientos de: instalación, reubicación de equipos y/o dispositivos de red/cómputo, servidores y sus servicios de internet, de bases de datos, del uso de la Intranet institucional, correo electrónico ,de control de acceso a los recursos, de requerimientos, etc.; así como reglamentos para el uso de la red, servicios, internet, sanciones, etc.

Por lo que a continuación se muestra un ejemplo de estas políticas de *cómo* deberán ser especificadas.

- **Del equipo**

De la instalación de equipo de cómputo.

1. Todo el equipo de cómputo (computadoras, estaciones de trabajo, supercomputadoras, y equipo accesorio), que esté o sea conectado a la Red- HCPT, o aquel que en forma autónoma se tenga y que sea propiedad de la Institución debe sujetarse a las normas y procedimientos de instalación que emite el Área de Redes del Departamento de TIC's de HCPT.

2. El Departamento de TIC's en coordinación con el departamento de Control de bienes deberá tener un registro de todos los equipos informáticos propiedad del HCPT.

3. El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en una área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales, la alimentación eléctrica, su acceso que el Departamento de TIC's tiene establecido en su normatividad de este tipo.

4. Los responsables de las áreas de apoyo Interno de los Departamentos deberán en conjunto con el área de Redes dar cabal cumplimiento a las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión.

5. La protección física de los equipos le corresponde a quienes en un principio se les asigne, y les corresponde notificar los movimientos en caso de que existan, a las autoridades correspondientes (departamento al que pertenece, departamento de TIC's, departamento de Control de bienes, y otros de competencia).

Del mantenimiento de equipo de cómputo.

1. Al área de informática del departamento de TIC's, le corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.

2. En el caso de los equipos atendidos por terceros el departamento de TIC's deberá normar al respecto.

3. El personal técnico de apoyo interno de los departamentos se apegará a los requerimientos establecidos en las normas y procedimientos que el área de Informática emita.

4. Los responsables de las áreas de Cómputo de un departamento pueden otorgar mantenimiento preventivo y correctivo, a partir del momento en que sean autorizados por el departamento de TIC's.

5. Corresponde al área de informática dar a conocer las listas de las personas, que puedan tener acceso a los equipos y brindar los servicios de mantenimiento básico, a excepción de los atendidos por terceros.

6. Por motivos de normatividad expedidos por el HCPT queda estrictamente prohibido dar mantenimiento a equipo de cómputo que no sea de propiedad de la institución.

De la actualización del equipo.

1. Todo equipo de cómputo (computadoras personales, estaciones de trabajo, supercomputadora y demás relacionados), y los de telecomunicaciones que sean propiedad del HCPT debe procurar que

sea actualizado tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

De la reubicación del equipo de cómputo.

1. La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos que el área de Informática emita para ello.

2. En caso de existir personal técnico de apoyo de los departamentos, éste notificará de los cambios tanto físicos como de software de red que realice al departamento de TIC's, y en su caso si cambiara de responsable (el equipo) al departamento de Control de bienes de la Dirección financiera. Notificando también los cambios de equipo inventariado (cambio de monitores, de impresoras etc.).

3. El equipo de cómputo a reubicar sea del HCPT o bien externo se hará únicamente bajo la autorización del responsable contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.

- **Del control de accesos**

Del acceso a áreas críticas.

1. El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta el departamento de TIC's.

2. En concordancia con la política de la institución y debido a la naturaleza de estas áreas se llevará un registro permanente del acceso de personal, sin excepción.

3. El Departamento de TIC's deberá proveer de la infraestructura de seguridad requerida con base a los requerimientos específicos de cada área.

4. Bajo condiciones de emergencia o de situaciones de urgencia, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

Del control de acceso al equipo de cómputo.

1. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

2. Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que el Departamento de TIC's emita.

3. Las áreas de cómputo de los departamentos donde se encuentre el equipo cuyo propósito reúna características imprescindibles y de misión

crítica, deberán sujetarse también a las normas que establezca el departamento de TIC's.

4. Los accesos a las áreas críticas deberán ser clasificados de acuerdo a las normas que dicte el Departamento de TIC's de común acuerdo con su Comité de Seguridad Informática.

5. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, el área de informática tiene la facultad de acceder a cualquier equipo de cómputo que no esté bajo su supervisión.

Del control de acceso local a la red.

1. El área de redes es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

2. El departamento de TIC's es el responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.

3. Dado el carácter unipersonal del acceso a la Red-HCPT, el área de redes verificará el uso responsable, de acuerdo al Reglamento para el uso de la red.

4. El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, equipo centralizado de procesamiento, etc.) conectado a la red es administrado por el área de redes.

5. Todo el equipo de cómputo que esté o sea conectado a la Red-HCPT, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, deben sujetarse a los procedimientos de acceso que emite el área de redes.

De control de acceso remoto.

1. El área de redes es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.

2. Para el caso especial de los recursos de equipo especializado de cómputo a terceros deberán ser autorizados por el departamento de TIC's o por las Autoridades Superiores de la Institución.

3. El usuario de estos servicios deberá sujetarse al Reglamento de uso de la Red-HCPT y en concordancia con los lineamientos generales de uso de Internet.

4. El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite el departamento de TIC's.

De acceso a los sistemas administrativos.

1. Tendrá acceso a los sistemas administrativos sólo el personal del HCPT que sea titular de una cuenta de acceso o bien tenga la autorización del responsable si se trata de personal de apoyo Administrativo o Técnico.

2. El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.

3. Tendrá acceso al sistema de información de la Dirección Administrativa sólo aquellos usuarios de Red-HCPT o externos autorizados por dicha Dirección.

4. La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la Red-HCPT y por las normas y procedimientos establecidos por el departamento de TIC's.

5. Los servidores de bases de datos administrativos son delicados, por lo que se prohíbe, el acceso de cualquier persona, excepto para el personal de el área de sistemas de información.

6. El control de acceso a cada sistema de información de la Dirección Administrativa será determinado por la unidad responsable de generar y procesar los datos involucrados.

De los servicios de Internet.

1. En concordancia con las leyes nacionales y bajo las disposiciones de las políticas generales de informática, el área de servicios de internet es la responsable de instalar y administrar el o los servidor(es). Es decir, sólo se permiten servidores de páginas autorizados, y servicios de correo electrónico y mensajería por el área de servicios de internet.

2. El área de servicios de internet deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de Bases de Datos, del uso de la Intranet Institucional, correo electrónico, así como las especificaciones para que el acceso a éstos sea seguro.

3. Los accesos a las páginas web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso a la Red-HCPT.

4. A los responsables de los servidores de Web les corresponde la verificación de respaldo y protección adecuada.

5. Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos que el área de servicios de internet en coordinación del área de sistemas de información.

6. El material que aparezca en la página de Internet del HCPT deberá ser aprobado por el departamento de TIC's, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

7. En concordancia con la libertad de investigación, se acepta que en la red del HCPT conectada a Internet pueda ponerse información individual sin autorización (siempre y cuando no contravenga las disposiciones que se aplican a las instituciones gubernamentales del estado), por ejemplo: páginas personales, pero deberá llevar el enunciado siguiente: "Las expresiones, opiniones o comentarios que aquí aparecen pertenecen al autor individual y no necesariamente al HCPT "; no debe llevar el logotipo oficial del HCPT y deberá siempre responder a un comportamiento profesional y ético.

8. Con referencia a la seguridad y protección de las páginas, así como al diseño de las mismas deberá referirse a las consideraciones de diseño de páginas electrónicas establecidas por el área de servicios de internet.

9. El área de red en coordinación con el área de servicios de internet tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información, y conservar información del tráfico.

- **De utilización de los recursos de la red**

1. Los recursos disponibles a través de la Red-HCPT serán de uso exclusivo para asuntos relacionados con las actividades sustantivas de la institución.

2. El área de redes es la responsable de emitir y dar seguimiento al Reglamento para el uso de la Red.

3. De acuerdo con las disposiciones del HCPT, corresponde a la unidad de redes administrar, mantener y actualizar la infraestructura de la Red-HCPT.

4. El Departamento de TIC's debe propiciar el uso de las tecnologías de la información con el fin de contribuir con las directrices de desarrollo gubernamentales de la Institución y la Provincia.

5. Dado el carácter confidencial que involucra el correo electrónico el Comité de informática del Centro emite su reglamentación.

- **Del Software**

<u>De la adquisición de software.</u>

1. En concordancia con la política de la institución, el Comité de Informática y el área de proyectos informáticos son los organismos oficiales del

Centro para establecer los mecanismos de procuración de sistemas informáticos.

2. Del presupuesto de los proyectos que se otorga a las diferentes áreas del HCPT una cantidad deberá ser aplicada exclusivamente para la adquisición de programas y/o sistemas con licencias, bajo la dirección del departamento de TIC's.

3. De acuerdo con el Programa Provincial de Informática, la Prefectura en conjunto con el Comité de Informática y la Dirección de TIC's, propiciará la adquisición de licencias de sistemas operativos y utilitarios por empleado y/o por licencias en volumen, o a su vez se establecerá la utilización de alternativas de software libre, denotando el proceso que implica el cambio de tecnología en adiestramiento, acoplamiento y soporte, para obtener los mejores resultados de costo y beneficios de acorde al plan de austeridad del gobierno de la república.

4. Corresponderá al Departamento de TIC's emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

5. De acuerdo a los objetivos globales del departamento de TIC's se deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.

6. En cuanto a la paquetería sin costo deberá respetarse la propiedad intelectual intrínseca del autor.

7. El Departamento de TIC's promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

8. El Departamento de TIC's promoverá el uso de sistemas programáticos que permitan la independencia de la institución a los proveedores.

De la instalación de software.

1. Corresponde al área de Informática emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

2. En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual.

3. El área de informática es la responsable de brindar asesoría y supervisión para la instalación de software informático, así mismo el área de Redes para el software de telecomunicaciones.

4. La instalación de software que desde el punto de vista del departamento de TIC's pudiera poner en riesgo los recursos e integridad de la institución no estará permitida.

5. Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).

6. La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento o anomalía al área de informática.

De la actualización del software.

1. La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo a la calendarización que anualmente sea propuesta por el área de informática.

2. Corresponde al Departamento de TIC's autorizar cualquier adquisición y actualización del software.

3. Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por el área de proyectos informáticos.

De la auditoría de software instalado.

1. El área de proyectos informáticos del departamento de TIC's del HCPT es la responsable de realizar revisiones periódicas para asegurar que sólo programaciones con licencia estén instaladas en las computadoras de la institución.

2. El área de proyectos informáticos propiciará la conformación de un grupo especializado en auditoría de sistemas de cómputo y sistemas de información.

3. Corresponderá al grupo especializado dictar las normas, procedimientos y calendarios de auditoría.

Del software propiedad de la institución.

1. Toda la programática (Códigos fuentes, binarios, documentación técnica, manuales, etc.) adquirida por la institución sea por compra, contratación, prácticas pre profesionales y/o profesionales, donación o sesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera.

2. El área de informática en coordinación con el departamento de Control de bienes deberá tener un registro de todos los paquetes de programación propiedad del HCPT.

3. Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos del HCPT se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.

4. Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.

5. Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.

6. Corresponderá al área de informática promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos.

7. El departamento de las TICs en conjunto con la Dirección de Procuraduría Síndica propiciará la gestión de patentes y derechos de creación de software propiedad de la institución.

8. El departamento de las TICs administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

Sobre el uso de otro tipo de software.

1. Cualquier software que requiera ser instalado para trabajar sobre la Red-HCPT deberá ser evaluado por el área de sistemas.

2. Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de la institución.

De la propiedad intelectual.

1. Corresponde al departamento de las TICs procurar que todo el software instalado en la Red-HCPT esté de acuerdo a la ley de propiedad intelectual a que dé lugar.

- **De supervisión y evaluación**

1. Cada uno de las áreas del departamento de las TICs donde esté en riesgo la seguridad en la operación, servicio y funcionalidad del departamento, deberá emitir las normas y los procedimientos que correspondan.

2. Las auditorías de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca el departamento de las TICs o el grupo especializado de seguridad.

3. Para efectos de que la institución disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la Internet e Intranet dispongan.

4. Los sistemas considerados críticos, deberán estar bajo monitoreo permanente.

- **Generales.**

1. Cada uno de los departamentos deberá emitir los planes de contingencia que correspondan a las actividades críticas que realicen.

2. Debido al carácter confidencial de la información, el personal del departamento de las TICs deberá conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

- **Sanciones**

1. Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por el departamento de las TICs.

2. Las sanciones pueden ser desde una llamada de atención o informar al usuario, hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

3. Corresponderá al Comité de Informática hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la institución.

4. Todas las acciones en las que se comprometa la seguridad de la Red-HCPT y que no estén previstas en esta política, deberán ser revisadas por la Prefectura, el departamento de las TICs y un Comité de Seguridad de Sistemas para dictar una resolución sujetándose al estado de derecho.

Por lo expuesto existen muchas situaciones y aspectos que deben ser normados, con reglamentos, procedimientos para dotar de seguridad a los bienes, recursos, información y personal del HCPT.

4.6. Seguridades de red

La mayor parte de servicios de seguridades como protección antivirus, Spam, contenidos, detección de intrusos ya han sido establecidos, pero necesitan fortalecerse para un mejor rendimiento y Seguridad de la red.

A continuación se detallan los lineamientos que se han tomado como principales y fundamentales dentro de las seguridades de los recursos de red del HCPT y se definen las aplicaciones de tipo hardware o software que se utilizan y el periodo de control y/o ejecución.

Directrices	Hardware	Software	Control y ejecución
Defensa de Amenazas			
Protección antivirus		Symantec Endpoint Protection	Diariamente
Filtrado de Tráfico	Switch Catalyst 3560-48PS Symantec Gateway Security		Semanal
Detección y prevención de intrusiones	Symantec Gateway Security		Semanal
Filtrado de contenidos	Symantec Gateway Security	Squid 2.6	Semanal
Comunicación segura			
Cifradas Virtual Private Network (VPN)	Symantec Gateway Security		Mensual
Secure Socket Layer (SSL)	Symantec Gateway Security		Mensual
Cifrado de archivos	No establecida	No establecida	No establecida
La confianza y la identidad			
Autenticación, autorización y cuentas (AAA)		Active directory FreeRadius	Diariamente
Control de admisión a la red (NAC)		Active directory FreeRadius	Diariamente

Directrices	Hardware	Software	Control y ejecución
Infraestructura de clave pública (PKI)	No establecida	No establecida	No establecida
Acceso Inalámbrico			
SSID Broadcast	Access Points	Descativado	Semanal
Filtrado de MAC Address	Access Points	Activado	Mensual
Claves WEP, WAP	Access Points	Activado	Mensual
Autenticación	Servidor	FreeRadius	Mensual
Mejores prácticas de la seguridad de redes			
Gestión de Redes	Switch Catalyst 3560-48PS Symantec Gateway Security	Wireshrak, y sniffers, para administración de redes	Quincenal
Evaluación y auditorías	Revision y chequeo	aplicaciones, licenciamiento	Semestral
Políticas			Bimestral
Puertos	Symantec Gateway Security	Aplciaciones	mensual
Suministro de energia Eléctrica	Planta eléctrica		mensual

Figura 99: Directrices de seguridad

4.7. Resumen de la propuesta

Plataforma Tecnológica

Nivel	Tecnología	Dispositivos
Núcleo	Fibra óptica, Categoría 6, Switch Capa3	Switch Cisco Catalyst 3560G-48PS
Distribución	Switch capa 3 Categoría 6	Switch Cisco Catalyst 3560G-48PS
Acceso	Inalámbrica	Access Point Orinoco AP-4000
Enlaces remotos	Inalámbrica	Potenciar los radios de comunicación

Tabla 50: Resumen de la Plataforma Tecnología

Switching

Dirección o Departamentos	Dirección IP Clase B	Máscara
Administrativo	172.16.0.0	255.255.255.224
Asociación de Empleados	172.16.0.32	255.255.255.224
Bodega y Talleres	172.16.0.64	255.255.255.224
Desarrollo Humano y Cultura	172.16.0.96	255.255.255.224
Financiero	172.16.0.128	255.255.255.224
Gobierno Provincial, Aula Virtual, Cooperativa	172.16.0.160	255.255.255.224
Planificación y Procuraduría Síndica	172.16.0.192	255.255.255.224
Producción	172.16.0.224	255.255.255.224
Recursos Hídricos	172.16.1.0	255.255.255.224
Relaciones Externas	172.16.1.32	255.255.255.224
Sala de Consejeros	172.16.1.64	255.255.255.224
Secretaría General, Sala de Choferes	172.16.1.96	255.255.255.224
Sistemas	172.16.1.128	255.255.255.224
Vías y Construcciones	172.16.1.160	255.255.255.224
Internet	172.16.1.192	255.255.255.248

Tabla 51: Resumen de VLANs para Switching

Ruteo

Protocolo de ruteo: RIP V2

Ruta Resumida: dirección de la red 172.16.0.0 con máscara 255.255.254.0

Redes Inalámbricas

Servicio	Configuración
SSID Broadcast	Desactivar
Filtrado de MAC	Activado
Claves de acceso	* WEP y WAP
Autenticación	FreeRADIUS

Tabla 52: Resumen de Servicios Inalámbricos

*Se da las 2 alternativas, ya que WAP no es soportado por muchos dispositivos, hasta cambiar todos los dispositivos a un mismo estándar.

Servicios Institucionales

- **Servicios de red**

Servicio	Servidor
Firewall	Symantec Gateway Security
Internet Compartido	Squid 2.78
Internet Compartido Provisional	Squid 2.78
Correo electrónico	Lotus Domino 7.01
Antivirus	Symantec EndPoint Protection 11
Controlador de Dominio	Active Directory
DNS	DNS Server

Tabla 53: Resumen de Servicios de red

- **Servicios de aplicaciones**

Servicio	Servidor
Adquisición de Materiales	base datos documentales de Lotus Domino
Sistema de Control de Recursos Humanos	Aplicación en Visual Studio con base datos de Oracle 10g
Sistema Médico Odontológico	Aplicación en Visual Studio con base datos de Oracle 10g
Sistema de Control de Proveedores	Aplicación en Visual Studio con base datos de Oracle 10g
Sistema Financiero FINANSG	Aplicación en Visual FOX 6 con base de datos de SQL 200 Server

Tabla 54: Resumen de Servicios de aplicaciones

- **Servicios por implementar**

Servicio	Servidor
RADIUS para autenticación de MAC Address	FreeRadius
Protocolo de la Configuración de Host Dinámico, asignación automáticas de IP	DHCP Server sobre y dispositivos de comunicación inalámbricos
Sistema de Administración de Trámites y Solicitudes	Lotus Domino 7.01
Sistema de Control de Combustibles	Aplicación en Visual Studio con base datos de Oracle 10g
Sistema de Control de bienes e inventario	Aplicación en Visual Studio con base datos de Oracle 10g
Sistema de Administración y Control de Soporte y Mantenimiento de Equipos	Aplicación en Visual Studio con base datos de Oracle 10g
Sistema de Administración y Control de Contratos y Obras	Aplicación en Visual Studio con base datos de Oracle 10g
Sistema de Precios Unitarios y Presupuestos	Aplicación en Visual Studio con base datos de Oracle 10g
Sistema de Mapas Virtuales	Aplicación en Java con base datos de Oracle 10g

Tabla 55: Resumen Servicios por Implementar

Calidad de Servicio

Aplicación	Valor IPP	Descripción del tráfico	% Ancho Banda
Ruteo IP	6	Para los protocolos de ruteo y comunicación de los datos	10
Voz	5	Para voz sobre IP	20
Video Interactivo	4	Para video conferencias	
Video continuo	4	para transmitir videos en línea	20
Datos de misión crítica	3	Tráfico de transacciones financieras o video conferencias	
Señalización de llamadas	3	Para la inicialización de llamadas	15
Datos transaccionales	2	Tráfico de transacciones de aplicaciones de base de datos como Recursos Humanos, Lotus domino, Oracle, etc. Para la navegación de computadores importantes	
Administración de red	2	Para programas y protocolos de administración de la red	15
Volumen de datos	1	Operación de sincronización y replicación de base de datos	
Minería de datos	1	Para procesos de búsqueda intensa de herramientas complejas	10
Mejor esfuerzo	0	Operación de sincronización y replicación de base de datos	10

Tabla 56: Resumen de la clasificación de tráfico de Calidad de Servicio

Codificación y nomenclatura de dispositivos de red

Factores	Codificación
Infraestructura Física	EC,PS,BT,PF,PI,CA
Direcciones o Departamentos	CU,SG,RE,FN,RH,SC,VC,PL,JU,PR,AD,SY,AE,CO,AV,BM,BC,GP,TA, BO,SN
Ubicación	PB,P1,P2,P3,P4,P5,P6,P7,TC,M1,M2,TG,TS
Tipo de Dispositivo	SV,PC,FW,SW,AP,SP,IM,RB,MD,LP,SG,OT
Acceso al Medio	FO,WL,CB,NC
Cantidad de dispositivos	000-999

Tabla 57: Resumen de la Nomenclatura de dispositivos de red

Políticas institucionales

Lineamientos	Nivel de acción
Del Equipo	
	De la instalación de equipo de cómputo.
	Del mantenimiento de equipo de cómputo.
	De la actualización del equipo.
	De la reubicación del equipo de cómputo.
Del control de accesos	
	Del acceso a áreas críticas
	Del control de acceso al equipo de cómputo
	Del control de acceso local a la red
	De control de acceso remoto
	De acceso a los sistemas administrativos.
	De los servicios de Internet (WWW).
De utilización de los recursos de la red	
Del Software	
	De la adquisición de software
	De la instalación de software
	De la actualización del software
	De la auditoría de software instalado
	Del software propiedad de la institución
	Sobre el uso de otro tipo de software.
	De la propiedad intelectual
De supervisión y evaluación	
Generales	
Sanciones	

Tabla 58: Resumen de las Políticas

Seguridades de red

Directrices	Hardware	Software
Defensa de Amenazas		
Protección antivirus		Symantec Endpoint Protection
Filtrado de Tráfico	Switch Catalyst 3560-48PS	
	Symantec Gateway Security	
Detección y prevención de intrusiones	Symantec Gateway Security	
Filtrado de contenidos	Symantec Gateway Security	Squid 2.6
Comunicación segura		
Cifradas Virtual Private Network (VPN)	Symantec Gateway Security	
Secure Socket Layer (SSL)	Symantec Gateway Security	
Cifrado de archivos	No establecida	No establecida
La confianza y la identidad		
Autenticación, autorización y cuentas (AAA)		Active directory
		FreeRadius
Control de admisión a la red (NAC)		Active directory
		FreeRadius
Infraestructura de clave pública (PKI)	No establecida	No establecida
Acceso Inalámbrico		
SSID Broadcast	Access Points	Descativado
Filtrado de MAC Address	Access Points	Activado
Claves WEP, WAP	Access Points	Activado
Autenticación	Servidor	FreeRadius
Mejores prácticas de la seguridad de redes		
Gestión de Redes	Switch Catalyst 3560-48PS	Wireshrak, y sniffers, para administración de redes
	Symantec Gateway Security	
Evaluación y auditorías	Revision y chequeo	aplicaciones, licenciamiento
Políticas		
Puertos	Symantec Gateway Security	Aplciaciones
Suministro de energia Eléctrica	Planta eléctrica	

Tabla 59: Resumen de las Seguridades de red

4.8. Estimación de costos

Con el fin de determinar el valor de inversión para la reingeniería de la infraestructura de red del Honorable Consejo Provincial de Tungurahua, a continuación se desglosa un costo referencial para el mejoramiento de los equipos de red, sistemas, servidores, conexiones remotas, equipo para el respaldo de suministro de energía, el cual ha sido tomado como base de proformas y ofertas solicitadas a proveedores de la localidad.

Para los equipos de red, servidores y equipos de protección de amenazas.

No.	Detalle	Descripción	Cantidad	Valor Total
1	Switchs CATALYST 3560 48 10/100/1000 T PoE +SFP	Equipos de conmutación que se utilizarán para el nivel de distribución en las dependencias remotas	2	8.800,00
2	Servidores para rack doble procesador, 4 gigas de memoria RAM, tarjetas de GigabitEthernet	Servidores para servicios de DHCP, Controladores de Dominio, DNS, y autenticación con Radius	2	10.200,00
3	Servidor de Internet, Tarjeta de red Gigabitethernet, Disco duro y Memoria RAM	Actualización del servidor proxy de internet	1	4.000,00
4	Firewall	Renovación del equipo de protección físico contra ataques.	1	3.500,00
		Total		**26.500,00**

Tabla 60: Propuesta de costos para mejoramiento de equipos de red

Para incrementar el rendimiento de conexiones las remotas en los puntos del Centro de Promociones y Servicios de la Provincia y las áreas de Bodega y

talleres se detallan dos alternativas para el mejoramiento de la comunicación

1ra opción, Conexiones inalámbricas de radiofrecuencia de 5.4GHz

No.	Detalle	Descripción	Cantidad	Valor Total
1	Sistema de transmisión de punto a punto, Canopy	Sistema de conexión remota utilizando radiofrecuencias	3	10.500,00
2	Permisos de operación de radiofrecuencias	Pago anual por permiso de utilización y funcionamiento de radioenlaces	1	500,00
		Total		**11.000,00**

Tabla 61: Propuesta de costos para enlaces remotos mediante radiofrecuencia

2da opción, Conexión mediante fibra óptica

No.	Detalle	Descripción	Cantidad	Valor Total
1	Sistema de conexión de fibra óptica	Conexión remota de gran velocidad	3	15.000,00
		Total		**15.000,00**

Tabla 62: Propuesta de costos para enlaces remotos mediante fibra óptica

Aquí describiremos que una de las grandes ventajas de la fibra óptica es la velocidad de procesamiento superior a cualquier tecnología lo que permite transacciones en tiempo real, obteniéndose que éste sea uno de los mejores medios de transmisión para el nivel de núcleo de toda la red. Pero una de las desventajas es el costo elevado en la adquisición e instalación de esta tecnología, y si se la aplica se debe tomar en consideración costos de mano de obra, para el tendido de este cable ya sea por postes o subterráneo.

Otros de los puntos principales descritos en el análisis fue la falta de un sistema de respaldo de energía eléctrica al momento de un apagón:

No.	Detalle	Descripción	Cantidad	Valor Total
1	Planta Eléctrica Servidores	Respaldo de suministro de energía eléctrica para servidores	1	7.500,00
		Total		**7.500,00**

Tabla 63: Propuesta de costos para el respaldo del suministro de energía eléctrica

Es así que se tiene el siguiente resumen de costos

Inversión para la reingeniería

No.	Descripción	Valor
1	Equipos red, servidores, y protección	26.500,00
2	Mejoramiento Conexiones remotas opción 1	10.500,00
3	Respaldo energía	7.500,00
	Total	**44.500,00**

Tabla 64: Resumen de la Inversión para La reingeniería

Si se desea utilizar la tecnología de fibra óptica se tendría un incremento aproximado del 10% que reflejaría en la calidad de la transmisión y rapidez en el acceso los servicios y recursos de la red

De esta manera se podrá dotar de una buena plataforma tecnológica que se acople a futuros requerimientos, tenga una vida útil de por lo menos 8 años y que se puedan instalar nuevas tecnologías de comunicación como Voz sobre IP para telefonía IP

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Demostración de la Hipótesis

"La reingeniería de la red informática del H. Consejo Provincial de Tungurahua contribuirá a mejorar la calidad de los servicios informáticos institucionales mediante el control de los siguientes factores claves: velocidad de procesamiento de las peticiones de red, ancho de banda de la red, redistribución de los recursos de red, protocolos de la Calidad de Servicios y planes de seguridad y de contingencias"

Para poder optimizar la velocidad del tráfico de red se lo podrá hacer mediante la clasificación de tráfico para la Calidad de Servicio, una vez implementados estos servicios de calidad se podrá compartir el tráfico y priorizarlo, de esta manera se podrá optimizar el ancho de banda de la red, también se ha presentado la manera de cómo se debería implementar la nueva tecnología de red, a los niveles de Núcleo, Distribución y Acceso para permitir una alto rendimiento de la red, confiabilidad, escalabilidad y

seguridad, así como la implementación y utilización de políticas informáticas, para el correcto uso y acceso de los recursos, información y servicios.

Otro factor que ayudará al rendimiento de la red es la velocidad de procesamiento interno del dispositivo Cisco Catalyst 3560G-48PS, la cual se detalla a continuación.

Características de rendimiento del Cisco Catalyst 3560G-48PS.

- Ancho de banda para transmitir 32Gbps
- Alta velocidad de transmisión basados en paquetes de 64-byte
- 38,7 Mpps – Millones de paquetes por segundo
- 128 MB de DRM
- 32 MB de Memoria Flash
- Configurable hasta 12,000 direcciones físicas MAC
- Configurable hasta 11,000 rutas Unicats
- Configurable hasta 1000 grupos IGMP y rutas Multicast
- Configurable Unidad máxima transmisión MTU hasta 9000 bytes
- Con un máximo tamaño de tramas Ethernet de 9018 bytes
- Para transición sobre puertos Gigabit Ethernet hasta 1546 bytes

Para la demostración de la hipótesis, se tendrá que aplicar toda la propuesta y evaluar los resultados, y compararlos, de esta manera se podrá saber si realmente se logró optimizar el rendimiento de la red.

Se ha logrado crear una subred en la red actual en el área de sistemas, sin tener que cambiar ninguna configuración especial, tan solo cambiando la máscara para el grupo de Sistemas, cuya dirección es 192.168.1.48/255.255.255.248, que equivale a un rango de 6 direcciones IP válidas, a la cual se denominó VLAN de prueba,

Esta VLAN está conformado por los servidores principales y se procedió a realizar un monitoreo del tráfico de red sobre esta VLAN, bajo los mismos parámetros especificados en el Análisis de tráfico de red del Capítulo 3, pero cambiando el mes, es decir, en la última semana del mes de junio, en el horario de las 9 a 10 de la mañana, y se aplica 2 ejemplos, del primer dia de la semana y todos los días de la semana, con lo cual tenemos los siguientes resultados

Para el primer día de la semana

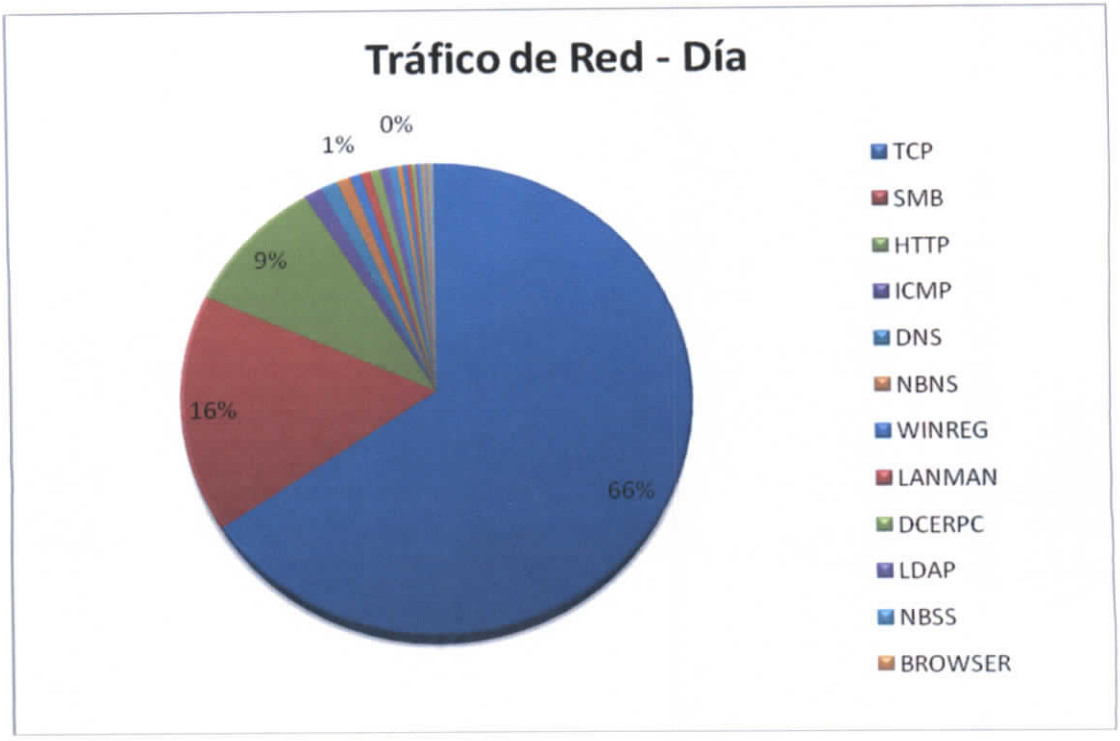


Figura 100: Porcentaje de tráfico de Red de un día para la Comprobación de la hipótesis

Siendo este el listado de los protocolos existentes en esta captura

Protocolos	Ocurrencias	Porcentaje
TCP	137397	66%
SMB	34207	16%
HTTP	19846	9%
ICMP	2556	1%
DNS	2262	1%
NBNS	1903	1%
WINREG	1486	1%
LANMAN	1372	1%
DCERPC	1357	1%
LDAP	1235	1%
NBSS	1143	1%
BROWSER	705	0%
KRB5	680	0%
DRSUAPI	578	0%
EPM	524	0%
CLDAP	430	0%
RPC_BROWSER	416	0%
LSA	372	0%
SAMR	296	0%
RPC_NETLOGON	254	0%
NTP	246	0%
ARP	142	0%
RIPv2	130	0%
IP	102	0%
RMI	10	0%
Socks	6	0%
DC=gov	6	0%
DPLAY	6	0%
SMB_NETLOGON	2	0%
UCP	1	0%
FF	1	0%
MDNS	1	0%
DC=ec'	1	0%

Tabla 65: Listado de protocolos del primer día

Y para toda la semana

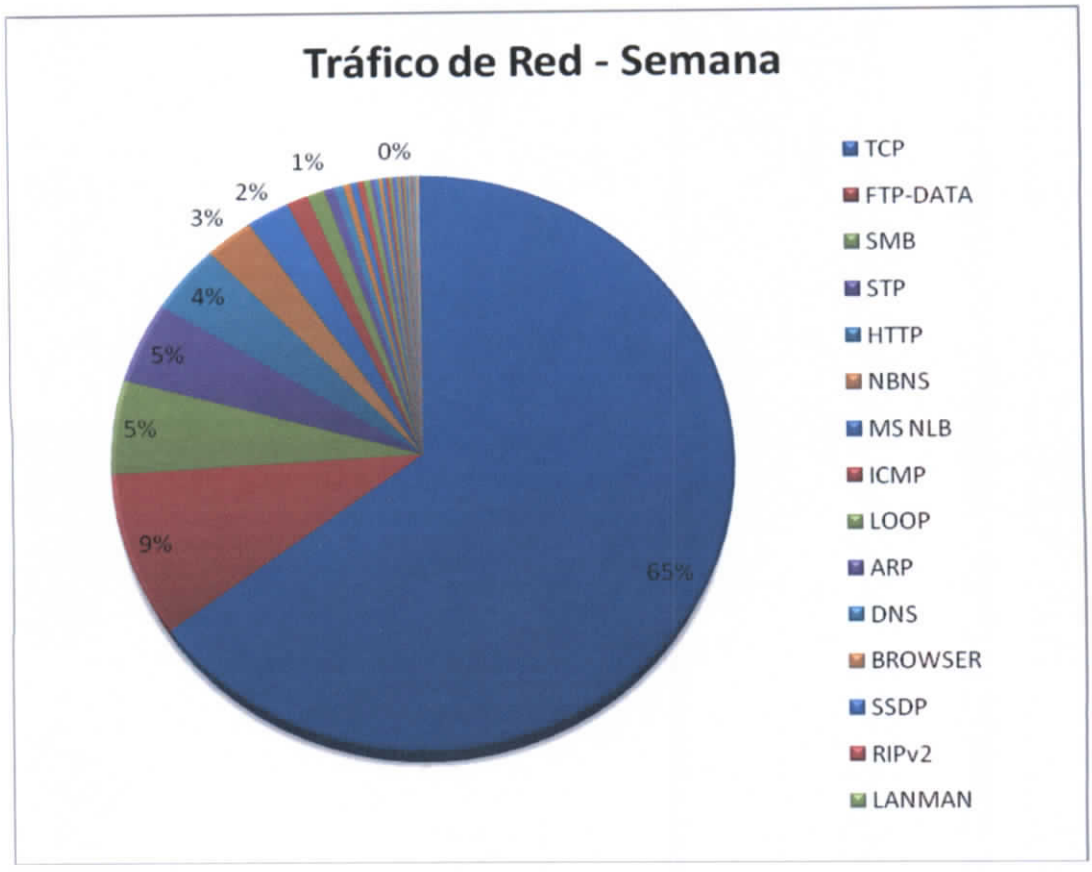


Figura 101: Porcentaje de tráfico de Red de una semana para la Comprobación de la hipótesis

Listado de los 10 primeros protocolos más representativos

Protocolo	Ocurrencia	Porcentaje
TCP	426238	65%
FTP-DATA	60528	9%
SMB	34828	5%
STP	30374	5%
HTTP	25704	4%
NBNS	17377	3%
MS NLB	15226	2%
ICMP	7721	1%
LOOP	6130	1%
ARP	3744	1%

Tabla 66: Listado de protocolos más representativos

De lo cual se puede obtener el siguiente resultado

ARP	Sin VLAN	Con VLAN	16 VLANS
Lunes	27%	0%	0%
Toda la Semana	40%	1%	16%

Tabla 67: Comparación de ARP

Explicación:

Sin la planeación de VLANs se tenían peticiones ARP de 40%, pero aplicando la VLAN de prueba se tiene que en una semana las peticiones son de 1%, asumiendo que se tenga implementado el esquema de VLANs para todas las 16 direcciones, el mismo tráfico tendría un promedio de 16%.

Con esta demostración se reduce en un 60% el tráfico de ARP y broadcast, para la red, haciendo que se optimice los servicios de la red y no se congestione.

Por lo tanto si se aplica el esquema propuesto de la reingeniería de red de este proyecto, que contiene los factores de Plataforma Tecnológica, Switching, Ruteo, Wireless, Calidad de Servicio, Políticas, las seguridades de red, nomenclatura y servicios se logrará obtener mejores resultados.

Probando de esta manera que la hipótesis planteada si se cumple

5.2. Conclusiones

Hoy en día el avance de las tecnologías de la comunicación nos permite estar conectados con nuestros seres queridos sin importar la distancia, realizando llamadas internacionales a bajos costos, lo que ha permitido el avance de sistemas de información, permitiendo estar más informados de los eventos que ocurren en el mundo entero en tan solo fracción de segundos, así lo podemos ver en noticieros internacionales; otro factor que ayuda a la comunicación son las video conferencias en tiempo real, que permiten interactuar como una llamada, o hasta recibir clases a larga distancia, todos estos procesos son totalmente transparentes para el usuario, no son muy complicados de manejarlos, ni de adquirirlos, pero el usuario no se percata del complicado proceso que hay debajo para realizar una conexión de llamada, para el envío de información, voz, datos y videos;, todo estos procesos y servicios están soportados por una red de datos.

Por lo tanto la red informática del H. Consejo Provincial de Tungurahua, es el eje principal de la tecnología de la comunicación e información, que ayuda a la toma de decisiones, gestionar proyectos de alcance social, sistematizar la información, desarrollar herramientas para el manejo de información de trabajo, automatizar procesos, y reducir recursos, logrando un mejor desempeño en las actividades que realiza esta organización, como por ejemplo transferencias inmediatas para pagos de obras, sistemas contables, sistemas de recursos humanos, consultas de presupuestos, materiales,

envío de informes, convenios internacionales, etc. De esta manera el HCPT informa al usuario sobre el desarrollo que realiza para el progreso de la provincia, en su sitio web.

Dentro del análisis realizado se detectó como factor principal que no existe un departamento o jefatura dedicada exclusivamente a la gestión de las tecnologías de la comunicación e información que permita gestionar, asesorar, planificar y ejecutar proyectos informáticos institucionales y provinciales, logrando de esta manera incrementar el desarrollo de las actividades que realiza el Consejo Provincial de Tungurahua, por su parte existe solamente una Unidad de Sistemas que no está debidamente potenciada y por el poco número de profesionales, no se pueden administrar ni dotar de un buen servicio de informática, ya que solo están apagando fuegos momentáneos en problemas triviales de los usuarios.

Es por esta condición y por la falta de decisión de las autoridades, que no se logra dar cumplimiento a los planes institucionales, menos a los planes informáticos, lo que conlleva a trámites burocráticos para dar solución a los problemas de congestión de los servicios de redes, y en lugar de ayudar a potenciar el área de sistemas, se crean en otros departamentos unidades de sistemas, dividiendo los planes de tecnología y creando diversos puntos que en lugar de dar una solución óptima, se agrega el desarrollo de las tecnologías de comunicación e información.

Entonces se plantea una solución para optimizar y proveer de los mecanismos necesarios al desarrollo de las tecnologías de comunicación e información que permitan acoplar futuros requerimientos y servicios institucionales, llevando consigo una mejor distribución de los recursos actuales, y un buen rendimiento en el flujo de la información clasificando por tipo de tráfico, además de un correcta aplicación de las normas y reglamentos para el usos de los recursos, información, servicios y capacitación del personal.

Hay que tener en cuenta que en cuestión de tecnología y desarrollo nunca se puede apostar a los servicios y productos de menor costo, para una gran innovación se requiere de una gran inversión que se verá reflejada en los beneficios a largo plazo, y podrá incrementar y automatizar los servicios y proyectos institucionales, en vez de estar "parchando" y "parchando" cuando se suscite algún problema, sería imprescindible proveer estos gastos y crear una buena plataforma tecnológica que tenga un tiempo de funcionamiento de por lo menos 8 años, pero hay que tener en consideración también que el avance de la tecnología se lo realiza diariamente, creando nuevos productos y servicios que incrementan la productividad de las empresas, por lo que un Departamento de Tecnologías de la Información y Comunicación centralizado y bien estructurado debería proveer un nivel de asesoramiento y gestión a los planes informáticos que vayan de la mano con los planes y proyectos institucionales.

5.3. Recomendaciones

Para poder tener una buena plataforma tecnológica para el desarrollo de los planes institucionales y provinciales se debe primeramente establecer un departamento que se encargue de administrar las tecnologías de la comunicación e información, entonces si por algo hay que empezar sería la conformación de este departamento con mas profesionales que se encarguen de controlar los servicios que se detallaron en la propuesta presentada de este proyecto de investigación.

Incrementar el presupuesto para las tecnologías, el cual debe ser sistemáticamente administrado y controlado por un departamento centralizado de tecnología de la Información y Comunicación y que en sus funciones principales estén las de planificar, desarrollar, ejecutar, controlar y validar proyectos informáticos, y que sean debidamente documentados, los mismos que deben acoplarse a los planes y proyectos de la institución y provincia y se conviertan en una plataforma principal de desarrollo.

También se deben cambiar los sistemas internos de manejo y control de las actividades, es decir cambiar el comportamiento de los procesos, para optimizar recursos, como tiempo, papel y dinero, sin dejar a un lado el potencial humano que a medida que evolucionan las tecnologías también debería de evolucionar su potencial intelectual.

Adicionalmente se requiere de una evaluación continua de los recursos, procesos, planes y proyectos informáticos, que permitan corregir y potenciarlos en su debido momento, y mantenerlos siempre en funcionamiento para que sean de fácil acceso y utilización para el usuario, y así de esta manera dotar de los mejores servicios al cliente final que es la comunidad tungurahuense a la cual sirve la Institución.

BIBLIOGRAFÍA

Libro de texto

Amato, Vito: *Academia de Networking de Cisco Systems: Guía del primer año*. Cisco Press, 2000. ISBN 1-57870-218-6

Amato, Vito: *Programa de la Academia de Networking de Cisco: Guía del segundo año*. Cisco Press, 2001. ISBN 1-578713-002-5.

Derfler, Frank: *Descubre redes LAN y WAN*. Prentice Hall, 1998. ISBN 84-8322-091-1

Ford, Merilee y Kim Lew, H.: *Tecnologías de interconectividad de redes*. Cisco Press, 1998. ISBN 970-17-0171-2.

Halsall, Fred.: *Comunicaciones de datos, redes de computadores y sistemas abiertos, 4ª Ed.* Addison-Wesley, 1998. ISBN 968-444-331-5

Kim Lew, H. y otros: *Interconectividad Manual para la Resolución de problemas*. Cisco Press, 2000. ISBN 970-17-0351-9.

Perlman, R.: *Interconnections Second Edition: Bridges, Routers, Switches and Internetworking Protocols*. Addison-Wesley, 2000. ISBN 0-201-63448-1.

Stallings, William: *Comunicaciones y Redes de Computadores, 6ª Ed.* Prentice Hall, 2000. ISBN 84-205-2986-9

Spohn, D.L.: *Data Network Design*, 2ª Ed. McGraw-Hill, 1997.

Teare, Diane.; Paquet, Catherine.: Campus Network Design Fundamentals, 2005, Cisco Press, ISBN: 1-58705-222-9

Tanenbaum, Andrew S.: *Redes de Computadoras, 3ª Ed.* Prentice-Hall, 1997. ISBN 968-880-958-6

Tanenbaum, Andrew S.: *Computer Networks, 4th Ed.* Prentice-Hall, 2003. ISBN 0-13-066102-3,

Historia

Hafner, K. y Lyon, M.: *Where Wizards stay up late. The Origins of the Internet*. Simon & Schuster, 1996.

Nivel físico

Black, Uyless: *Redes de ordenadores, protocolos, normas e interfaces, 2ª Ed.*,,1995.

Parnell, T.: *LAN Times Guía de redes de área extensa*. 1997. ISBN 84-481-1012-9.

Redes Locales

Held, G.: *LAN Performance. Issues and Answers. 2ª Ed*. Wiley, 1996.

Johnson, H. W.: *Fast Ethernet. Dawn of a new network*. Prentice Hall, 1996.

Seifert, R.*Gigabit Ethernet*. Addison-Wesley, 1998.

Routing

Habraken, Joe: *Routers Cisco. Serie Práctica*. Prentice Hall, 2000. ISBN 84-205-2952-4.

Huitema, C.: *Routing in the Internet*. Prentice Hall, 1995.

Shaugnessy, Tom y Velte, Toby: *Manual de CISCO*. McGraw-Hill, 2000. ISBN 84-481-2727-7.

TCP/IP

Comer, Douglas E.: *Redes Globales de información con Internet y TCP/IP. Vol. 1, 3ª Ed.* Prentice-Hall, 1996. ISBN 968-880-541-6.

Feit, Sidnie.: *TCP/IP. Arquitectura, protocolos e implementación, 2ª Ed.* Mc-Graw Hill. 1998. ISBN 84-481-1531-7.

Heywood, Drew: *Redes con Microsoft TCP/IP. Edición Especial, 3ª Ed.* Prentice Hall, 1999. ISBN 84-8322-108-X.

Huitema, C.: *IPv6. The New Internet Protocol.* Prentice Hall, 1996.

Miller, M. A. *Troubleshooting TCP/IP.* M&T Books, 1996.

Aplicaciones

Rose, M.T. y McCloghrie, K.: *How to Manage your Network Using SNMP.The Networking Management Practicum.* Prentice Hall, 1995.

Multimedia

Fluckiger, F.: *Understanding Networked Multimedia. Applications and Technology.* Prentice Hall, 1995.

Susbielle, J.: *Telefonía en Internet.* Eyrolles, 1996.

Seguridad

Cheswick, W.R. y Bellovin, S.M.: *Firewalls and Internet Security*, 1994.

Hafner, K. y Markoff, J.: *Cyberpunk. Outlaws and hackers on the Computer Frontier.* Simon & Schuster Inc., 1995.

Kaufman, C., Perlman, R. y Speciner, M.: *Network Security. Private Communication in a Public World.* Prentice Hall, 1995.

Online

- http://cw.prenhall.com/bookbind/pubbooks/stallings7/
- http://www.ciscopress.com/book.cfm?series=3&book=112
- http://www.cisco.com
- http://www.mundopc.net
- http://www.pchardware.org/redes/
- http://www.monografias.com
- http://www.wikipedia.org

GLOSARIO

A

AAA

En seguridad informática, AAA significa "la autenticación, autorización y contabilidad". La AAA es a veces combinada con la auditoría y en consecuencia se convierte en AAAA.

Autenticación

La autenticación se refiere al proceso de establecer la identidad digital de una entidad a otra entidad. Comúnmente una entidad es un cliente (un usuario, un ordenador cliente, etc.) y la otra entidad es un servidor (computadora).

Autorización

La mayor parte del tiempo la concesión de un privilegio constituye la capacidad de utilizar un determinado tipo de servicio. Ejemplos de los tipos de servicio incluyen, pero no se limitan a: la dirección IP de filtrado, la dirección destino, la ruta de sesión, QoS / servicios diferenciales, control de ancho de banda / gestión del tráfico, obligatorio túneles a un punto final, y el cifrado.

Contabilidad

Contabilidad se refiere al seguimiento del consumo de recursos de la red por los usuarios. Esta información puede ser utilizada para la gestión, planificación, facturación, u otros fines. En tiempo real de contabilidad se refiere a la información contable que se entrega simultáneamente con el consumo de los recursos. Lote de contabilidad se refiere a la información contable que se guarda hasta que sea entregado en un momento posterior. Típica información que se recoge en la contabilidad es la identidad del

usuario, la naturaleza del servicio prestado, cuando el servicio se inició, y cuando terminó.

ARP

ARP son las siglas en inglés de Address Resolution Protocol (Protocolo de Resolución de Direcciones).

Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de multidifusión de la red (broadcast (MAC = ff ff ff ff ff ff)) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto sólo funciona si todas las máquinas lo soportan.
ARP está documentado en el RFC (Request For Comments) 826.

El protocolo RARP realiza la operación inversa.
En Ethernet, la capa de enlace trabaja con direcciones físicas. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas).Para realizar ésta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC.

ARP se utiliza en 4 casos referentes a la comunicación entre 2 hosts:

1. Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.
2. Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.
3. Cuando un router necesita enviar un paquete a un host a través de otro router.
4. Cuando un router necesita enviar un paquete a un host de la misma red.

B

BOOTP

BOOTP son las siglas de Bootstrap Protocol. Es un protocolo de red UDP utilizado por los clientes de red para obtener su dirección IP automáticamente. Normalmente se realiza en el proceso de arranque de los ordenadores o del sistema operativo.

BROADCAST

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, sin necesidad de reproducir la misma transmisión nodo por nodo.

BROWSER

Un navegador web (del inglés, navigator o web browser) es una aplicación software que permite al usuario recuperar y visualizar documentos de hipertexto, comúnmente descritos en HTML, desde servidores web de todo el mundo a través de Internet. Esta red de documentos es denominada World Wide Web (WWW). Cualquier navegador actual permite mostrar o ejecutar gráficos, secuencias de vídeo, sonido, animaciones y programas diversos además del texto y los hipervínculos o enlaces.

C

Cable Categoría 6

Cable de Categoría 6, o Cat 6 (ANSI/TIA/EIA-568-B.2-1) es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es backward compatible (compatible con versiones anteriores) con los estándares de Categoría 5/5e y Categoría 3. La Categoría 6 posee características y especificaciones para crosstalk y ruido. El estándar de cable es utilizable

para 10BASE-T, 100BASE-TX y 1000BASE-TX (Gigabit Ethernet). Alcanza frecuencias de hasta 250 MHz en cada par.

El cable contiene 4 pares de cable de cobre trenzado, al igual que estándares de cables de cobre anteriores. Aunque la Categoría 6 está a veces hecha con cable 23 gauge, esto no es un requerimiento; la especificación ANSI/TIA-568-B.2-1 aclara que el cable puede estar hecho entre 22 y 24 gauge, mientras que el cable cumpla todos los estándares de testeo indicados. Cuando es usado como un patch cable, Cat-6 es normalmente terminado con conectores RJ-45, a pesar de que algunas cables Cat-6 son incómodos para ser terminados de tal manera sin piezas modulares especiales y esta práctica no cumple con el estándar. Si los componentes de los varios estándares de cables son mezclados entre sí, el rendimiento de la señal quedará limitado a la menor categoría que todas las partes cumplan.

Como todos los cables definidos por TIA/EIA-568-B, el largo máximo de un cable Cat-6 horizontal es de 90 metros (295 pies). Un canal completo (cable horizontal más cada final) está permitido a llegar a los 100 metros en extensión.

CDP

CDP (Cisco Discovery Protocol, 'protocolo de descubrimiento de Cisco') es un protocolo de red propietario de nivel 2, desarrollado por Cisco Systems y usado en la mayoría de sus equipos. Es utilizado para compartir información sobre otros equipos Cisco directamente conectados, tal como la versión del sistema operativo y la dirección IP.

CHAP

CHAP es un protocolo de autenticación por desafío mutuo (CHAP, en inglés: Challenge Handshake Authentication Protocol).

Es un método de autentificación remota o inalámbrica. Diversos proveedores de servicios emplean CHAP. Por ejemplo, para autentificar a un usuario frente a un ISP.
La definición de CHAP está contenida en la RFC 1994.

CHARGEN

Chargen (Generador de caracteres) es un programa informático para sistemas operativos basados en Unix que actúa de servidor de caracteres ofrecido por Inetd en el puerto 19 con los protocolos TCP y UDP.

Chargen es utilizado para comprobar el estado de algunas conexiones de red. El usuario remoto al ingresar a este puerto verá un listado de caracteres en formato ASCII que se repetirá de forma indefinida hasta que el mismo usuario finalice la conexión con el puerto.

CIDR

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. Su introducción permitió una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas. De esta manera permitió:

- Un uso más eficiente de las cada vez más escasas direcciones IPv4.
- Un mayor uso de la jerarquía de direcciones ('agregación de prefijos de red'), disminuyendo la sobrecarga de los enrutadores principales de Internet para realizar el encaminamiento.

CIDR es un estándar de red para la interpretación de 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.

CLDAP

Esta nota contiene una instantánea de la situación de la normalización de los protocolos utilizados en la Internet a partir del 17 de julio de 2001. Enumera protocolo oficial de las normas y las mejores prácticas actuales RFC; no es un índice completo de la serie RFC. La versión más reciente de este memo se designa ETS 1.

CSMA/CA

En las redes de computadoras, CSMA / CA pertenece a una clase llamada de protocolos múltiples métodos de acceso. CSMA / CA significa: Carrier Sense maca. En CSMA, una estación que desee transmitir primero tiene que escuchar el canal para un período de tiempo el fin de verificar para cualquier actividad en el canal. Si el canal está la sensación de "ociosos" y luego la estación está autorizada a transmitir. Si el canal es percibido como "ocupado" la estación tiene que aplazar su transmisión. Esta es la esencia de ambos CSMA / CA y CSMA / CD. En CSMA / CA (LocalTalk), una vez que el canal esta limpio, una estación envía una señal diciendo a las otras estaciones que no transmitan y, entonces envían sus paquetes. En Ethernet 802.3, la estación sigue esperando durante un tiempo, y chequean para ver si el canal está todavía libre. Si esta libre, la estación transmite, y espera una señal de confirmación de que el paquete fue recibido.

D

DCERPC

DCE Remote Procedure Call o bien DCE RPC es un sistema de llamada a procedimientos remotos del conjunto de software OSF DCE.1.
DCE RPC no debe confundirse con DCE el cual es un conjunto de servicios que incluye DCE RPC, además de otras cosas como CDS y DCE DFS.
DCE RPC fue encargado por la fundación Open Software Foundation. Una de las compañías clave que contribuyó fue Apollo.

DHCP

DHCP (sigla en inglés de Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

Diffserv

Este artículo es sobre servicios diferenciados dentro de las redes de comunicación. Para un concepto utilizado como patrón de diseño para aplicaciones de negocio (incluyendo servicios inteligentes y sensibles al contexto) ver servicios diferenciados (patrón de diseño).

DiffServ o Servicios diferenciados es una arquitectura de red de computadoras que específica una simple, escalable y de un amplio mecanismo para clasificar, gestionar el tráfico de la red y la prestación de Calidad de Servicio (QoS), garantizando una moderna red IP. DiffServ, por ejemplo, puede ser utilizado para proporcionar baja latencia, garantía de servicio (SG) para el tráfico de red críticos tales como la voz o el vídeo, al mismo tiempo provee una simple garantía de tráfico mayor-esfuerzo para servicios no críticos tales como el tráfico web o transferencias de archivos.

DNS

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

DoS Prevention

Denegación de Servicio (DoS) la prevención y dinámica de listas negras es utilizado por la SBC para bloquear parámetros maliciosos que atacan a la red.
La SBC debe vigilar el tráfico y señalización dinámica detectando posibles ataques sin perturbar el resto de los servicios que presta. Los ataques pueden entonces ser bloqueados internamente o externamente.

Los ataques DoS son ejecutados generalmente en servicios de Internet, para denegar estos servicios a otros. Ellos son usualmente encaminados al proveedor de servicios, y son meramente actos de vandalismo malintencionados o parte de un intento de extorsión.

DTP

DTP (Dynamic Trunk Protocol) es un protocolo que opera entre conmutadores, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

E

Echo (computación)

En términos de computación, echo tiene varias acepciones.

Por un lado es un servicio de red que repite aquel comando que se le envía (como el eco). Es útil para hacer comprobaciones sobre el estado de la conectividad de una red.
Por otro lado, Echo es un comando para la impresión de un texto en pantalla. Es utilizado en las terminales de los sistemas operativos como Unix, GNU/Linux, o MS-DOS; dentro de pequeños programas llamados scripts; y en ciertos lenguajes de programación tales como PHP.

F

FTP

FTP (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo.

G

GBIC

Un convertidor de interfaz gigabit (GBIC) es un estándar para transceptores, comúnmente usado con Gigabit Ethernet y Fibre Channel. Al ofrecer un estándar, intercambiables en caliente interfaz eléctrica, un puerto Ethernet Gigabit puede apoyar una amplia gama de medios físicos, de cobre a largo de onda de un solo modo de fibra óptica, con longitudes de cientos de kilómetros.

H

Hostname

Hostname es el programa que se utiliza para mostrar o establecer el nombre actual del sistema (nombre de equipo). Muchos de los programas de trabajo en red usan este nombre para identificar a la máquina. El NIS/YP también utiliza el nombre de dominio.
Cuando se invoca sin argumentos, el programa muestra los nombres actuales

HTTP

HTTP son las siglas de "Hyper Text Transfer Protocol" el cual es el principal protocolo tecnológico de la red que permite enlazar y navegar por Internet. Si no tuviéramos http, no podríamos acceder e interactuar en la red de redes como lo hacemos actualmente. Las cosas serían bastante más duras y confusas para todos.

HTTP-RPC-EPMAP

Este servicio detecta el http-rpc-epmap de conexión para el puerto 593 y procesa la memoria temporal de los datos recibidos al puerto 593. En este punto final se provee un mapeado de CIS (COM+ Internet Services) Este punto final de cartografía proporciona CIS (COM + Internet Services) y parámetros, como el puerto 135(epmap) de RPC.

I

ICMP

El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el subprotocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta ping y traceroute, que envían mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible, el tiempo que le toma a los paquetes en ir y regresar a ese host y cantidad de hosts por los que pasa.

IDS

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.
El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas

IEEE

IEE corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como Ingenieros Eléctricos, Ingenieros en Electrónica, Científicos de la Computación, Ingenieros en Informática e Ingenieros en Telecomunicación.

IGMP

El protocolo de red IGMP se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia.

IntServ

En las redes de computadoras, IntServ o servicios integrados es una arquitectura que especifica los elementos para garantizar la calidad de servicio (QoS) en redes. IntServ por ejemplo, puede ser utilizado para permitir video y sonido para llegar al receptor sin interrupción.

IntServ especifica un fino engranaje de sistema de QoS, que es a menudo contrastado con DiffServ del grueso engranaje del sistema de control.

La idea de IntServ es que cada router en el sistema implemente IntServ, y todas las aplicaciones que requiere algún tipo de garantías, tiene que hacer una reserva individual. "Especificaciones de Flujo" describe cual es para la reservación, al mismo tiempo "RSVP" es el mecanismo para señalarlo a través de la red.

IOS

IOS son las siglas de (Internetwork Operating System, Sistema Operativo de Interconexión de Redes) creado por Cisco Systems para programar y mantener equipos de interconexión de redes informáticas como switches (conmutadores) y routers (enrutadores).

IP Internet Protocol

Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI. Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar.

Es habitual que un usuario que se conecta desde su hogar a Internet utilice una dirección IP. Esta dirección puede cambiar al reconectar; y a esta forma de asignación de dirección IP se denomina una dirección IP dinámica (normalmente se abrevia como IP dinámica).

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija (se aplica la misma reducción por IP fija o IP estática), es decir, no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos, y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

A través de Internet, los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, a los seres humanos nos es más cómodo utilizar otra notación más fácil de recordar y utilizar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS.

Existe un protocolo para asignar direcciones IP dinámicas llamado DHCP (Dynamic Host Configuration Protocol).

IPFILTER

IPFilter (comúnmente denominado CIP) es un paquete de software que pueden utilizarse para proporcionar traducción de direcciones de red (NAT) o firewall. Puede ser utilizado como un módulo del kernel cargables (LKM) o incorporados en el Unix núcleo; uso como carga de módulos del núcleo cuando sea posible, es altamente recomendable. Scripts se prestan a instalar el parche y los archivos del sistema, según sea necesario. El autor y mantenedor es Darren Reed.

IPS

Un sistema de prevención de intrusiones es un dispositivo de seguridad que vigila la red y / o actividades del sistema de maliciosos o no deseados de comportamiento y puede reaccionar en tiempo real, para bloquear o impedir esas actividades.

IPSec

IPsec (abreviatura de Internet Protocol Security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

ITU

La Unión Internacional de Telecomunicaciones (ITU) es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

K

Kerberos

Kerberos es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura. Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro. Los mensajes de autenticación están protegidos para evitar intromisiones y ataques de Replay.

Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza. Además, existen extensiones del protocolo para poder utilizar criptografía de clave asimétrica.

Kpasswd

kpasswd – El comando kpasswd cambia la contraseña registrada en una base de datos de autenticación de entrada. De forma predeterminada, el intérprete de comandos cambia la contraseña de la AFS nombre de usuario que coincida con la del emisor identidad local (UNIX UID). Para especificar un usuario suplente, se incluye el principal argumento. El nombre de usuario por el principal argumento no tiene que aparecer en el archivo de contraseña local (el archivo */ etc / passwd* o equivalente), contraseña del emisor en la base de datos de autenticación.

L

LAN

LAN en informática designa a una red de área local, conocida por sus siglas en inglés LAN (Local Area Network).
Una red de área local, o red local, es la interconexión de varios ordenadores y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de hasta 100 metros. Su aplicación más extendida es la interconexión de computadores personales y estaciones de trabajo en

oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

LDAP

LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Habitualmente, almacena la información de login (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Login

"/login" tiene dos comportamientos: Como requeridor de credenciales y como aceptador de credenciales.
Si el cliente ya tiene una sesión "single sing-on" con FCAS, el navegador presentará a FCAS una cookie segura conteniendo una cadena identificando un "ticket-granting ticket". Está cookie es llamada "ticket-granting cookie". Si la cookie contiene un ticket "ticket-granting" valido, FCAS podrá entregar "tickets de servicio" a las aplicaciones registradas que los soliciten.

Lotus domino

El software IBM Lotus Domino ofrece excelentes funciones de colaboración que se pueden desplegar como una infraestructura central de planificación empresarial y de correo electrónico, como una plataforma de aplicaciones empresariales o como ambas cosas.

Lotus Domino y sus opciones de software de cliente ofrecen un entorno seguro y fiable de mensajería y colaboración que aumenta la productividad de las personas, agiliza los procesos empresariales y mejora la capacidad de respuesta de la empresa en general

Ventajas

- Amplía la mensajería con herramientas de colaboración integradas.

- Ofrece flexibilidad y variedad de plataformas de hardware, sistemas operativos, directorios y accesos de cliente.
- Proporciona funciones punteras de seguridad que protegen la información fundamental para la empresa.
- Disminuye el coste total de propiedad (TCO) al facilitar un uso eficaz de los recursos de CPU, el ancho de banda de red y el almacenamiento en disco.
- Maximiza la disponibilidad de servidor con agrupación en clúster avanzada, registro cronológico de transacciones, recuperación de errores de servidor y herramientas de diagnóstico automático.

Gracias a las funciones avanzadas de administración que incluye, reduce el tiempo y los costes asociados al despliegue y la gestión de la infraestructura. Soporta servicios web y estándares abiertos, y ofrece herramientas de integración con las aplicaciones existentes.
Puede proporcionar una rápida recuperación de las inversiones (ROI) gracias a las soluciones basadas en software Lotus Domino para procesos empresariales como la gestión de relaciones con los clientes, la cadena de suministros y el seguimiento de proyectos.

M

MAC

En redes de computadoras la dirección MAC (Medium Access Control address o dirección de control de acceso al medio) es un identificador de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el OUI. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64 las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación. Debido a esto, las direcciones MAC son a veces llamadas Quemadas en las Direcciones (BIA).

MAN

Una red de área metropolitana (En inglés, Metropolitan Area Network o MAN) es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado (MAN BUCLE), la tecnología de pares de cobre se posiciona como una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades que van desde los 2Mbps y los 155Mbps.

MDNS

Zeroconf o Zero Configuration Networking es un conjunto de técnicas que permiten crear de forma automática una red IP sin configuración o servidores especiales. También conocida como Automatic Private IP Addressing or APIPA, permite a los usuarios sin conocimientos técnicos conectar ordenadores, impresoras de red y otros elementos y hacerlos funcionar. Sin Zeroconf, un usuario con conocimientos técnicos debe configurar servidores especiales, como DHCP y DNS, o bien configurar cada ordenador de forma manual.

MDI

Los programas de ordenador gráficos de interfaz de múltiples documentos (MDI) son aquellos cuyas ventanas se encuentran dentro de una ventana padre (normalmente con la excepción de las ventanas modales), de manera opuesta a una interfaz de documento único. Se suele utilizar el acrónimo MDI. Ha habido muchos debates sobre qué tipo de interfaz se prefiere. Generalmente se considera que SDI es más útil si los usuarios trabajan con varias aplicaciones. Las compañías han utilizado ambos sistemas con reacciones diversas. Por ejemplo, Microsoft ha cambiado la interfaz de sus aplicaciones Office de SDI a MDI y luego otra vez a SDI, aunque el grado de implementación varía entre componentes.

MTA

Un agente de transferencia de correo (MTA) (también conocido como Agente de Transporte de Correo, Agente de Transferencia de Mensajes, o smtpd (corto para SMTP demonio)), es un programa de ordenador o software agente que transfiere mensajes de correo electrónico de un ordenador a otro.

El término servidor de correo también se utiliza en el sentido de un ordenador que actúa como un MTA que se está ejecutando el software adecuado. El término intercambiador de correo (MX), en el contexto del sistema de nombres de dominio se refiere formalmente a una dirección IP asignada a un dispositivo que aloja un servidor de correo, y por extensión también indica el propio servidor.

N

NAC

Network Access Control es un concepto de redes de computadoras y un conjunto de protocolos utilizados para definir la forma de conseguir los nodos de la red antes de acceder a los nodos de la red. NAC podría integrar el proceso de reparación automática (fijando las condiciones no conforme requeridas antes de permitir el acceso a nodos) en los sistemas de redes, permitiendo que la infraestructura de red tales como routers, switches y firewalls para trabajar junto con los servidores de back office y el equipo informático del usuario final para asegurar que el sistema de información este funcionando bien antes de la interoperabilidad permitida.

NAT

NAT (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

Existen muchas variantes de traducción de direcciones que se prestan a distintas aplicaciones. Sin embargo todas las variantes de dispositivos NAT deberían compartir las siguientes características:

- Asignación transparente de direcciones.
- Encaminamiento transparente mediante la traducción de direcciones (aquí el encaminamiento se refiere al reenvío de paquetes, no al intercambio de información de encaminamiento).
- Traducción de la carga útil de los paquetes de error ICMP

NBNS

Resolución de nombres de NetBIOS sobre TCP/IP y WINS.
NetBIOS sobre TCP/IP es el componente de red que realiza la resolución o asignación de nombres de nombre de equipo a dirección IP (NETBT.SYS en Windows NT, y VNBT.VXD en Windows para Trabajo en Grupo y Windows 95). Actualmente hay cuatro métodos de resolución de nombres de NetBIOS sobre TCP/IP: nodo b, nodo p, nodo m y nodo h.

NBSS

SAMBA es SMB/NetBIOS sobre TCP/IP. El protocolo NetBIOS utiliza tres puertos, a saber el servicio
> 137 (tcp y udp) para resolución de nombres (nbt)
> 139 (tcp y udp) para servicio de sesiones (nbss)
> 138 (tcp y udp) para servicio de datagramas (nbdgm).

NETBIOS

NetBIOS, "Network Basic Input/Output System", es, en sentido estricto una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico. NetBIOS fue originalmente desarrollado por IBM y Sytek como API/APIS para el software cliente de recursos de una Red de área local (LAN). Desde su creación, NetBIOS se ha convertido en el fundamento de muchas otras aplicaciones de red.

NNTPS

Las Noticias de la red de Protocolo de transferencia o NNTP es una aplicación de Internet protocolo utilizado principalmente para la lectura y publicación de artículos Usenet (alias netnews), así como la transferencia de noticias entre servidores de noticias.

NTP

Network Time Protocol (NTP) es un protocolo de internet para sincronizar los relojes de los sistemas informáticos a través de ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

O

OCSP

Online Certificate Status Protocol (OCSP) es un método para determinar el estado de revocación de un certificado digital X.509 usando otros medios que no sean el uso de CRL (Listas de Revocación de Certificados). Este protocolo se describe en el RFC 2560 y está en el registro de estándares de Internet.
Los mensajes OCSP se codifican en ASN.1 y habitualmente se transmiten sobre el protocolo HTTP. La naturaleza de las peticiones y respuestas de OCSP hace que a los servidores OCSP se les conozca como "OCSP responders".

Ventajas sobre las CRL
OCSP fue creado para solventar ciertas deficiencias de las CRL. Cuando se despliega una PKI (Infraestructura de Clave Pública), es preferible la validación de los certificados mediante OCSP sobre el uso de CRL por varias razones:
OCSP puede proporcionar una información más adecuada y reciente del estado de revocación de un certificado.

- OCSP elimina la necesidad de que los clientes tengan que obtener y procesar las CRL, ahorrando de este modo tráfico de red y procesado por parte del cliente.
- El contenido de las CRL puede considerarse información sensible, análogamente a la lista de morosos de un banco.

- Un "OCSP responder" puede implementar mecanismos de tarificación para pasarle el coste de la validación de las transacciones al vendedor, más bien que al cliente.
- OCSP soporta el encadenamiento de confianza de las peticiones OCSP entre los "responders". Esto permite que los clientes se comuniquen con un "responder" de confianza para lanzar una petición a una autoridad de certificación alternativa dentro de la misma PKI.

Una consulta sobre el estado de un certificado sobre una CRL, debe recorrerla completa secuencialmente para decir si es válido o no. Un "OCSP responder" en el fondo, usa un motor de base de datos para consultar el estado del certificado solicitado, con todas las ventajas y estructura para facilitar las consultas. Esto se manifiesta aún más cuando el tamaño de la CRL es muy grande.

OSPF

Open Shortest Path First (frecuentemente abreviado OSPF) es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible.

OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. Puede operar con seguridad usando MD5 para autentificar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Como sucesor natural de RIP, acepta VLSM o sin clases CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

Outlook

Microsoft Outlook o Outlook (nombre completo de Microsoft Office Outlook desde Outlook 2003) es un administrador de información personal de Microsoft, y es parte del Microsoft Office.

P

PAP

PAP son las siglas de Password Authentication Protocol, un protocolo simple de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un ISP. PAP es un sub-protocolo usado por la autenticación del protocolo PPP (Point to Point Protocol), validando a un usuario que accede a ciertos recursos. PAP transmite contraseñas o pasword en ASCII sin cifrar, por lo que se considera inseguro. PAP se usa como último recurso cuando el servidor de acceso remoto no soporta un protocolo de autenticación más fuerte.

PERSONAL COMPUTER

Una computadora personal (PC) es cualquier computadora cuyo precio de venta original, el tamaño y capacidad lo hacen especialmente útil para las personas, y que estén destinadas a ser explotadas directamente por un usuario final, sin intervención de operador de computadora.

Hoy en día un PC puede ser un ordenador de sobremesa, un ordenador portátil o un Tablet PC. Los más comunes son los sistemas operativos Microsoft Windows, Mac OS X y Linux, mientras que las más comunes son los microprocesadores x86 compatible CPU. Aplicaciones de software para ordenadores personales incluyen el tratamiento de textos, hojas de cálculo, base de datos, juegos, y una miríada de productividad personal y para fines especiales de software. Modernas computadoras personales a menudo de alta velocidad o conexiones de acceso telefónico a Internet, permitiendo el acceso a la World Wide Web y una amplia gama de otros recursos.

PKI

En criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a

veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.

PKIX-CRL

El protocolo de los convenios descritos en el presente documento satisface algunas de las necesidades operacionales de la Internet de la infraestructura de clave pública (PKI). Este documento especifica las convenciones para utilizar el Protocolo de transferencia de archivos (FTP) y el Protocolo de transferencia de hipertexto (HTTP) a la obtención de los certificados y revocación de certificados listas (CRL) de PKI repositorios. Mecanismos adicionales para abordar las necesidades operacionales de PKIX se especifican en documentos separados.

PoE

PoE (Power over Ethernet) es una tecnología que permite la alimentación eléctrica de dispositivos de red a través de un cable UTP / STP en una red Ethernet. PoE se rige según el estándar IEEE 802.3af y abre grandes posibilidades a la hora de dar alimentación a dispositivos tales como cámaras de seguridad, teléfonos o puntos de acceso inalámbricos.

POP3

Los proveedores de Internet en informática se utilizan el Post Office Protocol (POP3) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. La mayoría de los suscriptores acceden a sus correos a través de POP3.
Las versiones del protocolo POP (informalmente conocido como POP1) y POP2 se han hecho obsoletas debido a las últimas versiones de POP3. En general cuando uno se refiere al término POP, nos referimos a POP3 dentro del contexto de protocolos de correo electrónico.

PSI

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

PPPoE

PPPoE (Point-to-Point Protocol over Ethernet o Protocolo Punto a Punto sobre Ethernet) es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizada mayormente para proveer conexión de banda ancha mediante servicios de cable módem y xDSL. Este ofrece las ventajas del protocolo PPP como son la autenticación, cifrado y compresión.
En esencia, es un protocolo túnel, que permite implementar una capa IP sobre una conexión entre dos puertos Ethernet, pero con las características de software del protocolo PPP, por lo que es utilizado para virtualmente "marcar" a otra máquina dentro de la red Ethernet, logrando una conexión "serial" con ella, con la que se pueden transferir paquetes IP, basado en las características del protocolo PPP.

PPTP

(Point to Point Tunneling Protocol), es un protocolo desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.
Una VPN es una red privada de computadores que usa Internet para conectar sus nodos. PPTP ha sido crackeado o descifrado, no debería usarse donde la privacidad de los datos sea importante.

PUERTO DE RED

Un puerto de red puede ser un puerto serial o un puerto paralelo; suelen ser numerados. La implementación del protocolo en el destino utilizará ese número para decidir a qué programa entregará los datos recibidos.

Q

QoS

QoS o Calidad de Servicio (En inglés, Quality of Service) son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio.

R

RADIUS

RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

RMON

La Red Remote MON itoring (RMON) MIB fue desarrollado por la IETF para apoyar la vigilancia y el análisis de protocolo de LAN. La versión original (a veces denominado RMON1) se centró en la información de la Capa 1 y la Capa 2 del modelo OSI de redes Ethernet y Token Ring. Se ha prorrogado por RMON2 que incluye soporte para la capa de red y la capa de aplicación de vigilancia y SMON que incluye soporte para redes conmutadas. Se trata de una especificación estándar de la Industria que proporciona gran parte de la funcionalidad ofrecida por los analizadores de red. Los agentes RMON se incorporan en una gama alta de switches y routers (como los construidos por ProCurve, 3Com y Cisco).

RIP

RIP son las siglas de Routing Information Protocol (Protocolo de encaminamiento de información). Es un protocolo de puerta de enlace interna o IGP (Internal Gateway Protocol) utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

RS-232

RS-232 (también conocido como Electronic Industries Alliance RS-232C) es una interfaz que designa una norma para el intercambio serie de datos binarios entre un DTE (Equipo terminal de datos) y un DCE (Data Communication Equipment, Equipo de Comunicación de datos), aunque existen otras situaciones en las que también se utiliza la interfaz RS-232.

El puerto serie RS-232C, presente en todos los ordenadores actuales, es la forma más comúnmente usada para realizar transmisiones de datos entre ordenadores. El RS-232C es un estándar que constituye la tercera revisión de la antigua norma RS-232, propuesta por la EIA (Asociaci¢n de Industrias Electrónicas), realizándose posteriormente un versión internacional por el CCITT, conocida como V.24. Las diferencias entre ambas son mínimas, por lo que a veces se habla indistintamente de V.24 y de RS-232C (incluso sin el sufijo "C"), refiriéndose siempre al mismo estándar.

El RS-232C consiste en un conector tipo DB-25 de 25 pines, aunque es normal encontrar la versión de 9 pines DB-9, mas barato e incluso más extendido para cierto tipo de periféricos (como el serial del mouse del PC). En cualquier caso, los PCs no suelen emplear más de 9 pines en el conector DB-25. Las señales con las que trabaja este puerto serie son digitales, de +12V (0 lógico) y -12V (1 lógico), para la entrada y salida de datos, y a la inversa en las señales de control. El estado de reposo en la entrada y salida de datos es -12V. Dependiendo de la velocidad de transmisión empleada, es posible tener cables de hasta 15 metros.

RSA SEcur ID

RSA SecurID es un mecanismo desarrollado por RSA Security para realizar autenticación de dos factores para que un usuario de una red de recursos. El sistema de autentificación RSA SecurID® cuenta con la confianza de miles de organizaciones en todo el mundo para proteger los valiosos recursos de red. Utilizado conjuntamente con el RSA® Authentication Manager, un autentificador RSA SecurID funciona como una tarjeta ATM para una red, requiriendo que los usuarios se identifiquen con dos factores exclusivos – algo que conocen y algo que tienen – antes de permitirles el acceso. Millones de personas utilizan autentificadores RSA SecurID para acceder de forma segura a VPNs, puntos de acceso inalámbrico, cortafuegos de acceso remoto, aplicaciones de red y sistemas operativos de red. El sistema es fácil de utilizar y gestionar y tiene como consecuencia una mayor seguridad, lo cual puede proporcionar un rendimiento de la inversión más rápido en la mayoría de iniciativas de e-business.

RSVP

El Protocolo de reserva de recursos (RSVP), que se describe en el RFC 2205, es una empresa de transporte capa de protocolo destinado a reserva de recursos a través de una red de manera integrada los servicios de Internet. ICMPIGMPRFC 2205 "RSVP no aplicación de transporte de datos, pero es más bien un protocolo de control de Internet, como ICMP, IGMP, o protocolos de enrutamiento" - RFC 2205. multicastunicast RSVP proporciona receptor-inició la configuración de las reservas de recursos para multicast o unicast los flujos de datos con la expansión y solidez.

HostsroutersQoS RSVP puede ser utilizado por cualquier hosts o router para solicitar o entregar los niveles específicos de calidad de servicio (QoS) para la aplicación de datos corrientes. RSVP define cómo las aplicaciones a cabo las reservas y la forma en que pueden renunciar a los recursos reservados una vez que la necesidad de ellos ha llegado a su fin. Operación RSVP por lo general es el resultado de que los recursos se reserven a cada nodo a lo largo de un camino.

Routing protocol RSVP no es en sí misma un protocolo de enrutamiento y fue diseñado para interoperar con los actuales y futuros protocolos de enrutamiento.

Citation neededtraffic engineeringRSVP-TE RSVP es de por sí rara vez desplegados en redes de telecomunicaciones, pero la ingeniería de extensión de tráfico de RSVP, o RSVP-TE, es cada vez más ampliamente aceptada hoy en día en muchos QoS orientado a las redes.

RTSP

El protocolo de flujo de datos en tiempo real (del inglés Real Time Streaming Protocol) establece y controla uno o muchos flujos sincronizados de datos, ya sean de audio o de video. El RTSP actúa como un mando a distancia mediante la red RTSP es un protocolo no orientado a conexión, en lugar de esto el servidor mantiene una sesión asociada a un identificador, en la mayoría de los casos RTSP usa TCP para datos de control del reproductor y UDP para los datos de audio y vídeo aunque también puede usar TCP en caso de que sea necesario para servidores multimedia.

S

SFP

El pequeño forma-factor pluggable (SFP) es un compacto, "hot-pluggable" transceptor óptico utilizado en comunicaciones ópticas, tanto para las telecomunicaciones y comunicaciones de datos. Se trata de un formato de una industria popular apoyado por varios componentes de fibra óptica de los proveedores.

Transceptores SFP están destinados a apoyar SONET, Gigabit Ethernet, canal de fibra, y otras comunicaciones. La norma se está expandiendo a la SFP + que será capaz de soportar velocidades de hasta 10,0 Gbps (que incluyen la velocidad de transmisión de datos para el canal de fibra de 8 Gbits, y 10GbE. SFP + módulo para las versiones óptica, así como el cobre, se está introduciendo.

SMB

Server Message Block o SMB es un Protocolo de red (que pertenece a la capa de aplicación en el modelo OSI) que permite compartir archivos e impresoras (entre otras cosas) entre nodos de una red. Es utilizado principalmente en ordenadores con Microsoft Windows y DOS.

SMTP

Simple Mail Transfer Protocol (SMTP), o Protocolo Simple de Transferencia de Correo. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

SNMP

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento

SOCKET

Socket designa un concepto abstracto por el cual dos programas (posiblemente situados en computadoras distintas) pueden intercambiarse cualquier flujo de datos, generalmente de manera fiable y ordenada.

SPAM

Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de internet que han sido objeto de correo basura incluyen grupos de noticias, usenet, motores de búsqueda, wikis, foros, blogs, también a través de popups y todo tipo de imágenes y textos en la web. El correo basura también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea como por ejemplo Outlook, Lotus Notes, etc.

SSDP

Simple Servicio Discovery Protocol (SSDP) es una versión anterior del proyecto IETF de Internet de Microsoft y Hewlett-Packard. SSDP es la base del descubrimiento del protocolo Universal plug-and-play.
SSDP proporciona un mecanismo que los clientes de la red pueden utilizar para descubrir los servicios de red. Los clientes pueden utilizar SSDP con poca o ninguna configuración estática.

SSID

El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Existen algunas variantes principales del SSID. Las redes ad-hoc, que consisten en máquinas cliente sin un punto de acceso, utilizan el BSSID (Basic Service Set Identifier); mientras que en las redes en infraestructura que incorporan un punto de acceso, se utiliza el ESSID (E de extendido). Nos podemos referir a cada uno de estos tipos como SSID en términos generales. A menudo al SSID se le conoce como nombre de la red.

Uno de los métodos más básicos de proteger una red inalámbrica es desactivar el broadcast del SSID, ya que para el usuario medio no aparecerá como una red en uso. Sin embargo no debería ser el único método de defensa para proteger una red inalámbrica. Se deben utilizar también otros sistemas de cifrado y autentificación.

SSL

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes.

STP

STP, acrónimo de Shielded Twisted Pair o FUTP Par Trenzado Apantallado. El cable de par trenzado apantallado es justamente lo que su nombre implica: cables de cobre aislados dentro de una cubierta protectora, con un número específico de trenzas por pie. STP se refiere a la cantidad de aislamiento alrededor del conjunto de cables y, por lo tanto, a su inmunidad al ruido al contrario que UTP (Unshielded Twisted Pair, "Par trenzado sin apantallar") que no dispone de dicho aislamiento.

SYMANTEC NAC 5,1

Con Symantec la adquisición de Sygate a finales de 2005, la empresa de seguridad adquirida conocimientos y herramientas que han permitido continuar con nuevas áreas de productos. Por cuestiones de seguridad asociados, la más importante la descendencia de la unión es Symantec Network Access Control (SNAC), una línea de software y hardware para redes de ofertas de casi cualquier tamaño.

En su forma más básica, 5,1 SNAC es un producto de software único que combina un servidor de administración con el agente basado en la tecnología para hacer cumplir de punto final y bloquear las políticas o reparar los sistemas que no cumplen. Para construcción VARs de redes de mayor tamaño, Symantec ofrece tres aparatos que proporcionan LAN, puerta de enlace y física DHCP aplicación de la política.

CRN Test Center miró a los ingenieros de software de aplicación sólo de SNAC, que consistió en la Symantec Sygate Policy Manager, una aplicación agente, Sygate firewall personal y un servidor DHCP de software plug-in. La instalación del producto es relativamente sencilla, pero los instaladores deben planificar la aplicación del producto y no sólo de buceo en el asistente de instalación. Una comprensión básica del diseño de red y puntos finales es una obligación de garantizar una instalación sin complicaciones.

El gestor de la política componente está instalado en un servidor Windows 2003 y tiene varios otros requisitos previos (al igual que la mayoría de los productos NAC), como por ejemplo Internet Information Services y World Wide Web Services y, por supuesto, debe cumplir con los requisitos mínimos de hardware se indica en la guía de inicio . En aras de la simplicidad, Centro de pruebas, los ingenieros instalan el gestor de la política y sus componentes en un único servidor. El producto del asistente de configuración del servidor hizo corto trabajo de la instalación real, y la documentación incluida de inicio rápido demostrando ser un excelente recurso para la instalación.

SNAC política del gerente organiza la red de grupos sobre la base de los departamentos, ubicaciones y así sucesivamente. Sitios más pequeños por lo general pueden obtener de un único grupo mundial de gestión de las políticas. El corazón del producto es su seguridad las políticas, donde los administradores definen el punto final de requisitos y medidas que deban tomarse. Política de creación y gestión es bastante fácil, en parte gracias a una interfaz de gestión concisa, amplia ayuda en línea y una amplia documentación.

SYSLOG

syslog es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

Un mensaje de registro suele tener información sobre la seguridad del sistema, aunque puede contener cualquier información. Junto con cada mensaje se incluye la fecha y hora del envío.

T

TCP

TCP (Transmission Control Protocol, en español Protocolo de Control de Transmisión) es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 - 1974 por Vint Cerf y Robert Kahn. Muchos programas dentro de una red de datos compuesta por ordenadores pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP, SSH y FTP.

Funciones de TCP

En la pila de protocolos TCP/IP, TCP es la capa intermedia entre el protocolo de internet (IP) y la aplicación. Habitualmente, las aplicaciones necesitan que la comunicación sea fiable y, dado que la capa IP aporta un servicio de datagramas no fiable (sin confirmación), TCP añade las funciones necesarias para prestar un servicio que permita que la comunicación entre dos sistemas se efectúe: libre de errores, sin pérdidas y con seguridad.

TELNET

Telnet (TELecommunication NETwork) es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

TFTP

TFTP son las siglas de Trivial file transfer Protocol (Protocolo de transferencia de archivos triviales). Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Windows o cualquier otro cliente ligero que arrancan desde un servidor de red.

TLS

Secure Sockets Layer (SSL) y Transport Layer Security (TLS) -Seguridad de la Capa de Transporte-, su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras en Internet. Existen pequeñas diferencias entre SSL 3.0 y TLS 1.0, pero el protocolo permanece sustancialmente igual. El término "SSL" según se usa aquí, se aplica a ambos protocolos a menos que el contexto indique lo contrario.

U

UDP

User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

UPS

Un sistema de alimentación ininterrumpida (UPS), también conocida como una continua fuente de alimentación (CPS) o una batería es un dispositivo que mantiene un suministro continuo de energía eléctrica para el equipo conectado mediante el suministro de energía de una fuente de suministro de energía eléctrica cuando no está disponible. Se diferencia de un auxiliar de alimentación o generador de espera, que no ofrece protección instantánea de una interrupción momentánea de energía. Sistemas integrados que tienen UPS y generan reserva de componentes son a menudo denominados sistemas de energía de emergencia.

UUCP

UUCP es una abreviatura de Unix to Unix Copy. El término generalmente se refiere a un conjunto de programas de ordenador y protocolos que permiten la ejecución remota de comandos y la transferencia de archivos, correo electrónico y en concreto, uucp es uno de los programas en la suite, que proporciona una interfaz de usuario para solicitar las operaciones de copia de archivos.

UUCP La suite también incluye uux (interfaz de usuario para la ejecución remota de comandos), uucico (programa de comunicación), uustat (informes estadísticos sobre la actividad reciente), uuxqt (ejecutar comandos enviados

desde las máquinas remotas), y uuname (informes uucp el nombre del sistema local).

Aunque UUCP fue desarrollado originalmente por la mayoría y está estrechamente relacionada con Unix, existen implementaciones de UUCP para varios otros sistemas operativos, incluyendo Microsoft, MS-DOS, Digital VAX / VMS, Commodore's AmigaOS, y Mac OS.

V

VLAN

Una VLAN (acrónimo de Virtual LAN, 'red de área local virtual') es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de colisión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador).

Una 'VLAN' consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo cable, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de ninguna reconfiguración hardware.

VNC

VNC son las siglas en inglés de Virtual Network Computing (Computación en Red Virtual). VNC es un programa de software libre basado en una estructura cliente-servidor el cual nos permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente. También llamado software de escritorio remoto. VNC permite que el sistema operativo en cada computadora sea distinto: Es posible compartir la pantalla de una máquina

de "cualquier" sistema operativo conectando desde cualquier otro ordenador o dispositivo que disponga de un cliente VNC portado.

VPN

La Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.
Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un Hotel. Todo ello utilizando la infraestructura de Internet.

W

WAN

Una Red de Área Amplia (En inglés, Wide Area Network o WAN), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a un País o un Continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible). Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes.

WAP

Wireless Application Protocol o WAP (protocolo de aplicaciones inalámbricas) es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, p.ej. acceso a servicios de Internet desde un teléfono móvil.

Se trata de la especificación de un entorno de aplicación y de un conjunto de protocolos de comunicaciones para normalizar el modo en que los dispositivos inalámbricos, se pueden utilizar para acceder a correo electrónico, grupo de noticias y otros.
El Organismo que se encarga de desarrollar el estándar WAP fue originalmente el WAP Forum, fundado por cuatro Empresas del sector de las

comunicaciones móviles, Sony-Ericsson, Nokia, Motorola y Openwave (originalmente Unwired Planet). Desde 2002 el WAP Forum es parte de la Open Mobile Alliance (OMA), consorcio que se ocupa de la definición de diversas normas relacionadas con las comunicaciones móviles, entre ellas las normas WAP.

WEP

WEP, acrónimo de Wired Equivalent Privacy, es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, por lo que son más susceptibles de ser captadas por cualquiera que las redes cableadas. Cuando fue presentado en 1999, el sistema WEP fue requerido para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

WINS

Windows Internet Naming Service (WINS) es un servidor de nombres de Microsoft para NetBIOS, que mantiene una tabla con la correspondencia entre direcciones IP y nombres NetBIOS de ordenadores. Esta lista permite localizar rápidamente a otro ordenador de la red.

Al usar un servidor de nombres de internet de windows en una red se evita el realizar búsquedas más laboriosas (como peticiones broadcast) para obtenerla, y se reduce de esta forma el tráfico de la red.

A partir de Windows 2000 WINS ha sido relegado en favor de DNS y Active Directory, sin embargo, sigue siendo necesario para establecer servicios de red con versiones anteriores de sistemas Microsoft.

WIRELESS

La comunicación inalámbrica (inglés wireless, sin cables) es el tipo de comunicación en la que no se utiliza un medio de propagación físico alguno esto quiere decir que se utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio *físico* que comunique

cada uno de los extremos de la transmisión. En ese sentido, los dispositivos físicos sólo están presentes en los emisores y receptores de la señal, como por ejemplo: Antenas, Laptops, PDAs, Teléfonos Celulares, etc.

802

802.1D

802.1D es el estándar de IEEE para bridges MAC (puentes MAC), que incluye bridging (técnica de reenvío de paquetes que usan los switches), el protocolo Spaning Tree y el funcionamiento de redes 802.11, entre otros.

802.1P

IEEE 802.1p es un estándar que proporciona priorización de tráfico y filtrado multicast dinámico. Esencialmente, proporciona un mecanismo para implementar Calidad de Servicio (QoS) a nivel de MAC (Media Access Control).

802.1Q

El protocolo IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

802.1x

802.1x utiliza tres términos que usted necesita saber. El usuario o cliente que quiere ser autenticado se llama un suplicante. El servidor actual que hace la autenticación, normalmente un servidor RADIUS, se llama el servidor de autenticación. Y el dispositivo en un punto intermedio, como un punto de acceso inalámbrico, se llama el autenticador.

Uno de los puntos clave del 802.1x es que el autenticador puede ser simple y mudos de todos los cerebros tienen que estar en el suplicante y el servidor de autenticación. Esto hace que 802.1x sea ideal para puntos de acceso inalámbricos, que suelan ser pequeñas y tienen poca memoria y potencia de procesamiento.

802.11

El protocolo IEEE 802.11 o Wi-Fi es un estándar de protocolo de comunicaciones del IEEE que define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.

802.11i

El 802.11i se ratificó el 24 de junio de 2004 para abordar el problema de la seguridad en redes inalámbricas. Se basa en el algoritmo de cifrado TKIP, como el WPE, pero también admite el AES (Estándar de cifrado avanzado) que es mucho más seguro.

WiFi Alliance creó una nueva certificación, denominada WPA2, para dispositivos que admiten el estándar 802.11i (como ordenadores portátiles, PDA, tarjetas de red, etc.).

A diferencia del WPA, el WPA2 puede asegurar tanto las redes inalámbricas en modo infraestructura como también redes en modo "ad hoc".

802.3ab

1000Base-T, recogido en la revisión IEEE 802.3ab, es un estándar para redes de área local del tipo Gigabit Ethernet sobre cable de cobre trenzado sin apantallamiento. Fue aprobado por el IEEE 802.3 en 1999.

802.3af

Es el estándar de Power Over the Ethernet, PoE permite la entrega de energía DC sobre el mismo cable de cobre de Ethernet, esto permite la posibilidad de integrar nuevos dispositivos de energía adjuntos a la red a su

infraestructura LAN existente, evitando así el tendido de cable de energía o el uso de fuentes de alimentación para alimentar los dispositivos. Entre los dispositivos que pueden alimentarse utilizando PoE podemos encontrarnos Puntos de Acceso (APs), Camaras IP y telefonos IP entre otros.

802.3u

802,3 IEEE es una colección de IEEE normas definir la capa física, y el control de acceso a medios (MAC) sublayer de la capa de enlace de datos, cable de Ethernet. Esto es generalmente una LAN con algunas tecnologías WAN. Son conexiones físicas entre nodos y / o infraestructura de dispositivos (hubs, switches, routers) de distintos tipos de cobre o cable de fibra. 802,3 es una tecnología que puede apoyar la IEEE 802,1 arquitectura de red.

INDICE

ANEXOS

Anexo1: Inventario de equipos informáticos y dispositivos de red

#	Tipo	Direccion	IP	HOST	PC	SSID	MAC	p	p15	p16	p14	p13	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12
1	ADSL	Sistemas	200.107.35.65	MT800			00-0F-A3-1C-04-54	21	23	25	80	110	119	139	443	512	513	514	554				
2	FIREWALL	Sistemas	200.107.35.68				00-D0-68-0D-1B-D4	21	23	25	80	110	119	139	443	512	513	514	554				
3	FIREWALL	Sistemas	192.168.1.1	sgs.hcpt.gov.ec	Symantec Gateway Security 1600 Series (v3.0.1)		00-D0-68-0D-1B-D3	21	23	25	53	80	110	119	139	416	417	443	481	512	513	514	554
4	SERVIDOR	Sistemas	192.168.1.2	sunfv120.hcpt.gov.ec	SFV120		00-03-BA-2A-95-72																
5	SERVIDOR	Sistemas	192.168.1.3	sunf280r.hcpt.gov.ec	SF280R		00-03-BA-23-EB-F4	81	110	111	443	513	514	540	898								
6	SERVIDOR	Sistemas	192.168.1.4	mail.tungurahua.gov.ec	SF440		00-14-4F-4C-88-75	23	25	110	111	139	445	513	514								
7	PC	Secretaria	192.168.1.5	secretariapref.hcpt.gov.ec	SECRETARIAPREF	HCPT_SEC_G1	00-20-A6-58-4E-11	21	25	110	135	139	445										
8	PC	Secretaria	192.168.1.6	secgeneral.hcpt.gov.ec	secgeneral@tungurahua.gov.ec	HCPT_SEC_G1	00-20-A6-58-4D-DC	21	25	110	135	139	445										
9	PC	Secretaria	192.168.1.7	nancy.hcpt.gov.ec	NANCY	HCPT_SEC_G1	00-06-4F-31-BC-B9	21	25	110													
10	PC	Relaciones Externas	192.168.1.10	prensa.hcpt.gov.ec	PRENSA	HCPT_SEC_G1	00-40-F4-E6-92-BB	21	25	110	135	139	445										
11	ACCESS POINT	Secretaria	192.168.1.11	ORiNOCO-AP-4000-5d-68-c4	AP-4000 v3.1.0(1052) SN-05UT46600424 v3.1.0	HCPT_SEC_G1	00-20-A6-5D-68-C4	21	23	25	80	110											
12	PC	Secretaria	192.168.1.12	jefearchivo.hcpt.gov.ec	JEFEARCHIVO		00-13-20-CC-F8-76	21	25	110	135	139	445										
13	PC	Sala Consejeros	192.168.1.13	consejero	secre		00-08-A1-31-6A-E9	21	25	110													
14	PC	Sala Consejeros	192.168.1.14	consejeros.hcpt.gov.ec	consejeros	HCPT_RRHH_G1	00-06-4F-34-88-D5	21	25	110													
15	ACCESS POINT	Relaciones Externas	192.168.1.15	ORiNOCO-AP-4000-5d-68-a0	AP-4000 v3.1.0(1052) SN-05UT46600412 v3.1.0	HCPT_REX_G1	00-20-A6-5D-68-A0	21	23	25	80												
16	PC	Secretaria	192.168.1.16	prefecto.hcpt.gov.ec	PREFECTO		00-07-E9-3C-D5-07	21	25	110													
17	PC	Cooperativa	192.168.1.17	cooperativa.hcpt.gov.ec	COOPERATIVA	extreme1	00-20-A6-58-3C-A2	21	25	110													
18	PC	Secretaria	192.168.1.18	archivo1.hcpt.gov.ec	ARCHIVO1		00-13-20-CC-FB-40	21	25	110	139	445											
19	PC	Juridico	192.168.1.20	direccionj.hcpt.gov.ec	DIRECCIONJ	HCPT_PLAN_G1	00-20-A6-58-50-57	21	25	110	135	139	445										
20	PC	Juridico	192.168.1.22	secretariaj.hcpt.gov.ec	SECRETARIAJ	HCPT_PLAN_G1	00-20-A6-58-50-5E	21	25	110	135	139	445										
21	PC	Relaciones Externas	192.168.1.23	secrerree.hcpt.gov.ec	SECRERREE	HCPT_SEC_G1	00-06-4F-30-EC-0D	21	25	110	135	139	445										
22	PC	Juridico	192.168.1.24	abogacia.hcpt.gov.ec	ABOGACIA	HCPT_PLAN_G1	00-20-A6-58-50-70	21	25	110	135	139	445										
23	PC	Relaciones Externas	192.168.1.27	dirrelaexternas.hcpt.gov.ec	DIRRELAEXTERNAS	HCPT_REX_G1	00-06-4F-31-BD-89	21	25	110	139	445											

24	PC	Relaciones Externas	192.168.1.28	PRENSA2	PRENSA2	HCPT_REX_G1	00-40-F4-E6-92-C3	21	25	110	139	445																			
25	PC	Administrativo	192.168.1.30	direccionadm.hcpt.gov.ec	DIRECCIONADM	HCPT_ADM_G1	00-20-A6-57-ED-E1	21	25	110	135	139	445																		
26	PC	Administrativo	192.168.1.32	secretariaadm.hcpt.gov.ec	SECRETARIAADM	HCPT_ADM_G1	00-20-A6-57-ED-DA	21	25	110	135	139	445																		
27	PC	Administrativo	192.168.1.33	medico1.hcpt.gov.ec	medico1	HCPT_ADM_G1	00-12-17-8A-C5-6E	21	25	110																					
28	PC	Administrativo	192.168.1.34	apersonal.hcpt.gov.ec	APERSONAL	HCPT_ADM_G1	00-20-A6-57-EE-2B	21	25	110	135	139	445																		
29	PC	Administrativo	192.168.1.35	servadmin.hcpt.gov.ec	SERVADMIN	HCPT_ADM_G1	00-12-17-8A-C5-3D	21	25	110	135	139	445																		
30	PC	Administrativo	192.168.1.36	jefpersonal.hcpt.gov.ec	JEFPERSONAL	HCPT_ADM_G1	00-20-A6-57-ED-E3	21	25	110	135	139	445																		
31	RELOJ	Administrativo	192.168.1.37	HP-2000			00-64-00-00-0F-11	21	25	110	1001																				
32	PC	Administrativo	192.168.1.39	odontologico.hcpt.gov.ec	ODONTOLOGICO	HCPT_ADM_G1	00-20-A6-58-3C-AB	21	25	110	135	139	445																		
33	PC	Administrativo	192.168.1.40	trabajosocial1.hcpt.gov.ec		HCPT_ADM_G1	00-12-17-8A-C4-47	21	25	110	139	135	445																		
34	PC	Administrativo	192.168.1.41	serviciosadm.hcpt.gov.ec	SERVICIOSADM	HCPT_ADM_G1	00-20-A6-58-3C-B3	7	9	13	17	19	21	25	53	80	110	135	139	443	445										
35	PC	Administrativo	192.168.1.42	recaudador.hcpt.gov.ec	RECAUDADOR	HCPT_DHC_G1	00-20-A6-57-EE-2C																						
36	PC	Administrativo	192.168.1.45	enfermeria.hcpt.gov.ec	ENFERMERIA	HCPT_ADM_G1	00-20-A6-58-3B-CA	21	25	110																					
38	PC	Administrativo	192.168.1.47	apersonal2.hcpt.gov.ec	APERSONAL2	HCPT_ADM_G1	00-20-A6-57-EE-06	21	25	110	135	139	445																		
39	PC	Administrativo	192.168.1.48	salachoferes.hcpt.gov.ec	SALACHOFERES	HCPT_ADM_G1	00-12-17-8A-C4-9C	21	25	110																					
40	PC	Administrativo	192.168.1.49	electrico.hcpt.gov.ec	ELECTRICO	HCPT_ADM_G1	00-12-17-8A-C4-27	21	25	110																					
41	SERVIDOR	Sistemas	192.168.1.50	serversystem.hcpt.gov.ec	SERVERSYSTEM		00-08-A1-4A-11-1B	21	25	42	53	80	88	110	119	135	139	389	443	445	464	563	593								
42	ACCESS POINT	Administrativo	192.168.1.51	ORiNOCO-AP-4000-5b-6f-52	AP-4000 v3.2.1(1105) SN-05UT43560201 v3.1.0	HCPT_ADM_G1	00-20-A6-5B-6F-52	21	23	25	80	110																		
43	PC	Sistemas	192.168.1.52	systems.hcpt.gov.ec	SYSTEMS		00-19-D1-6A-3C-77	21	25	110	135	139	445																		
44	PC	Sistemas	192.168.1.55	programacion.hcpt.gov.ec	Progrmacion	HCPT_ADM_G1	00-20-A6-58-3B-D4	21	25	110	135	139	445																		
45	PC	Sistemas	192.168.1.56	database.hcpt.gov.ec	DATABASE	HCPT_ADM_G1	00-20-A6-57-ED-E0	21	25	110	135	139	445																		
46	PC	Sistemas	192.168.1.58	descargas.hcpt.gov.ec	DESCARGAS		00-08-A1-72-80-F4	25	110	135	139	445																			
47	ACCESS POINT	Speed Spectrum	192.168.1.60	TEW-430APB 802.11g Wireless Access Point		extreme1	00-40-F4-B8-C0-9A	21	25	80	110																				
48	ACCESS POINT	Speed Spectrum	192.168.1.61	TEW-430APB 802.11g Wireless Access Point		extreme1	00-40-F4-B9-35-7F	21	25	80	110																				
49	ACCESS POINT	Speed Spectrum	192.168.1.62	TEW-430APB 802.11g Wireless Access Point		extreme2	00-40-F4-B9-32-7A	21	25	80	110																				
50	ACCESS POINT	Speed Spectrum	192.168.1.63	TEW-430APB 802.11g Wireless Access Point		extreme2	00-40-F4-B8-C0-F6	21	25	80	110																				

51	ACCESS POINT	Speed Spectrum	192.168.1.64	AP_BOD_B1		HCPT_BOD_B1	00-02-6F-3C-56-83	21	25	80	110																
52	ACCESS POINT	Speed Spectrum	192.168.1.65	AP_BOD_B2		HCPT_BOD_B1	00-02-6F-3C-52-0C	21	25	80	110																
53	ACCESS POINT	Speed Spectrum	192.168.1.66	AP_BOD_B3		HCPT_BOD_B1	00-02-6F-3C-52-16	21	25	80	110																
54	ACCESS POINT	Bodega	192.168.1.67	ORiNOCO-AP-4000-5b-98-1c	AP-4000 v3.1.0(1052) SN-05UT43570221 v3.1.0	HCPT_BOD_G1	00-20-A6-5B-98-1C	21	23	25	80	110															
55	RELOJ	Talleres	192.168.1.68	HP-2000			00-64-00-00-29-A6	21	25	110	1001																
56	PC	Financiero	192.168.1.70	PYOLANDA	PYOLANDA	HCPT_FIN_G1	00-12-17-8A-C3-1B	21	25	110	135	139	445														
57	ACCESS POINT	Financiero	192.168.1.71	ORINOCO-AP-4000-59-c7-0f	AP-4000 v2.6.0(914) SN-05UT20600120 v3.1.0	HCPT_FIN_G1	00-20-A6-59-C7-0F	21	23	25	80	110															
58	PC	Financiero	192.168.1.72	CMSF_ROLES2	CMSF_ROLES2	HCPT_FIN_G1	00-12-17-8A-C3-0C	21	25	110																	
59	PC	Financiero	192.168.1.74	SERVIDOR	SERVIDOR		00-08-A179-DC-F4	21	25	110																	
60	ACCESS POINT	Financiero	192.168.1.77	Linksys WAP54G		HCPT_FIN_G2	00-12-17-7B-14-4E	21	25	80	110																
61	PC	Financiero	192.168.1.78	SACUNIA	SACUNIA	HCPT_FIN_G2	00-08-A1-9B-27-88	21	25	110	135	139	445														
62	PC	Financiero	192.168.1.80	MARTHACATUTA	MARTHACATUTA	HCPT_FIN_G2	00-08-A1-9B-2A-28	21	25	110	139	445															
63	PC	Financiero	192.168.1.82	MERCYSANCHEZ	MERCYSANCHEZ	HCPT_FIN_G2	00-08-A1-9B-29-D5	21	25	110	135	139	445														
64	PC	Financiero	192.168.1.84	ICALVACHE	ICALVACHE	HCPT_FIN_G2	00-08-A1-9B-27-87	21	25	110	135	139	445														
65	PC	Financiero	192.168.1.86	PATIQUINTANA	PATIQUINTANA	HCPT_FIN_G2	00-08-A1-9B-29-EE	21	25	110	139	445															
66	SERVIDOR	Financiero	192.168.1.87	servidordf.hcptdf.df	SERVIDORDF		00-14-C2-60-06-2F	21	25	53	88	110	135	389	464	593	636										
67	PC	Financiero	192.168.1.88	MANDRADE	MANDRADE	HCPT_FIN_G1	00-12-17-8A-C8-B7	21	25	110	135	139	445														
68	IMPRESORA	Financiero	192.168.1.91	FX-261840	FX-261840		08-00-37-26-18-40	21	25	110																	
69	PC	Financiero	192.168.1.92	SRICONTA3	SRICONTA3	HCPT_FIN_G1	00-12-17-8A-C5-B1	21	25	110	135	139	445														
70	PC	Financiero	192.168.1.94	SUSANAVACA	SUSANAVACA	HCPT_FIN_G1	00-08-A1-9B-27-8D	21	25	110	135	139	445														
71	PC	Financiero	192.168.1.96	DFPC14	DFPC14	HCPT_FIN_G1	00-08-A1-9B-28-63	21	25	110	139	445															
72	PC	Financiero	192.168.1.98	DFPC012	DFPC012	HCPT_FIN_G1	00-08-A1-9B-29-EA	21	25	110	139	445															
73	PC	Financiero	192.168.1.99	SROBAYO1	SROBAYO1	HCPT_FIN_G2	00-08-A1-9B-2A-18	21	25	110	139	445															
74	PC	Financiero	192.168.1.100	SROBAYO	SROBAYO	HCPT_FIN_G2	00-12-17-8A-C7-D6	21	25	110	139	445															
75	PC	Financiero	192.168.1.102	BHGB_CONTA5	BHGB_CONTA5	HCPT_FIN_G2	00-12-17-8A-C4-70	21	25	110																	
76	PC	Bodega	192.168.1.104	bodega2.hcpt.gov.ec	BODEGA2	HCPT_BOD_G1	00-20-A6-58-3C-48	21	25	110	135	139	445														

77	PC	Bodega	192.168.1.106	bodega3.hcpt.gov.ec	BODEGA3	HCPT_BOD_G1	00-20-A6-58-3B-D3	21	25	110	135	139	445										
78	PC	Bodega	192.168.1.107	bodega1.hcpt.gov.ec	BODEGA1	HCPT_BOD_G1	00-20-A6-58-3C-AD	21	25	110	135	445											
79	PC	Cultura	192.168.1.110	dircultuta.hcpt.gov.ec	DIRCULTURA	HCPT_DHC_G1	00-20-A6-58-4E-13	21	25	110	135	139	445										
80	ACCESS POINT	Cultura	192.168.1.111	ORiNOCO-AP-4000-5b-25-ce	AP-4000 v3.1.0(1052) SN-05UT41600096 v3.1.0	HCPT_DHC_G1	00-20-A6-5B-25-CE	21	23	25	80	110											
81	PC	Cultura	192.168.1.112	promotores2.hcpt.gov.ec	PROMOTORES2	HCPT_DHC_G1	00-20-A6-58-4E-4A	21	25	110													
82	PC	Cultura	192.168.1.114	promotores.hcpt.gov.ec	PROMOTORES	HCPT_DHC_G1	00-20-A6-58-4E-47	21	25	110	135	445											
83	PC	Cultura	192.168.1.117	secretariadhc.hcpt.gov.ec	SECRETARIADHC	HCPT_DHC_G1	00-20-A6-58-4D-D8	21	25	110	135	139	445										
84	PC	Cultura	192.168.1.118	promotores1.hcpt.gov.ec	PROMOTORES1	HCPT_DHC_G1	00-20-A6-58-4E-4E	21	25	110													
85	PC	Cultura	192.168.1.119	biblioteca.hcpt.gov.ec	biblioteca	HCPT_SEC_G1	00-20-A6-60-F2-7D	21	25	110													
86	PC	Planificacion	192.168.1.120	dirplanificacion.hcpt.gov.ec	DIRPLANIFICACION	HCPT_PLAN_G1	00-20-A6-58-4E-56	21	25	110													
87	ACCESS POINT	Planificacion	192.168.1.121	ORiNOCO-AP-4000-5b-69-5c	AP-4000 v3.1.0(1052) SN-05UT43600419 v3.1.0	HCPT_PLAN_G1	00-20-A6-5B-69-5C	21	23	25	80	110											
88	PC	Planificacion	192.168.1.122	secretariaplan.hcpt.gov.ec	SECRETARIAPLAN	HCPT_PLAN_G1	00-20-A6-58-4E-40	21	25	110	135	139	445										
89	PC	Planificacion	192.168.1.124	proyectos.hcpt.gov.ec	proyectos	HCPT_PLAN_G1	00-20-A6-58-4E-3C	21	25	110													
90	PC	Planificacion	192.168.1.125	olguitalaptop	olguitalaptop	HCPT_PRO_G1	00-14-A5-EE-36-26	21	25	110													
91	PC	Planificacion	192.168.1.126	descentralizar.hcpt.gov.ec	DESCENTRALIZAR	HCPT_PRO_G1	00-20-A6-58-4E-14	21	25	110	135	139	445										
92	PC	Planificacion	192.168.1.128	plantel.hcpt.gov.ec	PLANTEL	HCPT_PRO_G1	00-20-A6-58-50-58	21	25	110	135	139	445										
93	PC	Planificacion	192.168.1.131	gestion.hcpt.gov.ec	GESTION	HCPT_PLAN_G1	00-20-A6-58-4E-54	21	25	110	135	139	445										
94	PC	Planificacion	192.168.1.132	JSCHLAPTOP	JSCHLAPTOP	HCPT_PLAN_G1	00-12-F0-9B-AE-27	21	25	110													
95	PC	Recursos Hidricos	192.168.1.140	direccionrrhh.hcpt.gov.ec	DIRECCIONRRHH	HCPT_RRHH_G1	00-20-A6-54-4A-77	21	25	110	135	139	445										
96	ACCESS POINT	Recursos Hidricos	192.168.1.141	ORiNOCO-AP-4000-5b-25-dd	AP-4000 v3.1.0(1052) SN-05UT41600101 v3.1.0	HCPT_RRHH_G1	00-20-A6-5B-25-DD	21	23	25	80	110											
97	PC	Recursos Hidricos	192.168.1.142	secretariarrhh.hcpt.gov.ec	SECRETARIARRHH	HCPT_RRHH_G1	00-20-A6-54-4A-AE	21	25	110	135	139	445										
98	PC	Recursos Hidricos	192.168.1.144	diseniorrhh.hcpt.gov.ec	DISENIORRHH	HCPT_RRHH_G1	00-20-A6-58-3C-AC	21	25	110	135	139	445										
99	PC	Recursos Hidricos	192.168.1.145	pasantiarrhhh.hcpt.gov.ec	PASANTIARRHH	HCPT_RRHH_G1	00-20-A6-60-F2-58	21	25	110	135	139	445										
100	PC	Recursos Hidricos	192.168.1.146	disenioprograma.hcpt.gov.ec	DISENIOPROGRAMA	HCPT_RRHH_G1	00-20-A6-54-4B-11	21	25	110													
101	IMPRESORA	Recursos Hidricos	192.168.1.147	NPIF057F5	DesignJet 800PS (C7780C)		00-11-0A-F0-57-F5	21	25	110													
102	PC	Recursos Hidricos	192.168.1.148	jfiscal1.hcpt.gov.ec	JFISCAL	HCPT_RRHH_G1	00-20-A6-58-3B-C1	21	25	110													

103	PC	Recursos Hidiricos	192.168.1.149	fiscal4rrhh	fiscal4rrhh	HCPT_RRHH_G1	00-20-A6-58-3C-20	21	25	110	139	445											
104	PC	Recursos Hidiricos	192.168.1.150	fiscal1rrhh.hcpt.gov.ec	FISCAL1RRHH	HCPT_RRHH_G1	00-20-A6-58-3B-FD	21	25	110													
105	PC	Recursos Hidiricos	192.168.1.152	fiscal2rrhh.hcpt.gov.ec	fiscal2rrhh	HCPT_RRHH_G1	00-20-A6-58-3B-FC	21	25	110	135	139	445										
106	PC	Recursos Hidiricos	192.168.1.153	toporrhh.hcpt.gov.ec	TOPORRHH	HCPT_RRHH_G1	00-20-A6-58-3C-A1	21	25	110													
107	PC	Recursos Hidiricos	192.168.1.154	computorrhh.hcpt.gov.ec	computorrhh	HCPT_RRHH_G1	00-20-A6-58-8E-4D	21	25	110													
108	PC	Recursos Hidiricos	192.168.1.158	FISCAL3RRHH	FISCAL3RRHH	HCPT_RRHH_G1	00-20-A6-58-4D-F2	21	25	110													
109	PC	Recursos Hidiricos	192.168.1.159	PASANTESRRHH																			
110	PC	Recursos Hidiricos	192.168.1.161	jmedioambiente.hcpt.gov.ec	JMEDIOAMBIENTE	HCPT_RRHH_G1	00-20-A6-58-50-72	21	25	110													
111	PC	Recursos Hidiricos	192.168.1.162	gambiental1.hcpt.gov.ec	GAMBIENTAL1	HCPT_RRHH_G1	00-20-A6-54-4B-53	21	25	110													
112	PC	Recursos Hidiricos	192.168.1.164	AMBIENTE	AMBIENTE	HCPT_RRHH_G1	00-20-A6-58-3B-AA	21	25	110	139												
113	PC	Producción	192.168.1.170	dirproduccion.hcpt.gov.ec	DIRPRODUCCION	HCPT_PLAN_G1	00-20-A6-58-4E-7B	21	25	110	135	139	445										
114	ACCESS POINT	Producción	192.168.1.171	ORiNOCO-AP-4000-62-52-db		HCPT_PRO_G1	00-20-A6-62-52-DB																
115	PC	Producción	192.168.1.172	SECRETARIAPROD	SECRETARIAPROD	HCPT_PLAN_G1	00-20-A6-58-3B-D1	21	25	110	135	139											
116	PC	Producción	192.168.1.174	empresavial.hcpt.gov.ec	EMPRESAVIAL	HCPT_PRO_G1	00-20-A6-58-4E-76	21	25	110	135	139	445										
117	PC	Producción	192.168.1.176	pirt.hcpt.gov.ec	PIRT	HCPT_PRO_G1	00-20-A6-58-4E-79	21	25	110	135	139	445										
118	PC	Producción	192.168.1.178	agropecuario.hcpt.gov.ec	AGROPECUARIO	HCPT_PRO_G1	00-20-A6-60-82-C9	21	25	110													
119	PC	Producción	192.168.1.180	desarrollo2.hcpt.gov.ec	DESARROLLO2	HCPT_PRO_G1	00-20-A6-58-4E-46	21	25	110													
120	PC	Producción	192.168.1.182	mmora.hcpt.gov.ec	MMORA	HCPT_PRO_G1	00-20-A6-58-4E-6A	21	25	110	135	139	445										
121	PC	Producción	192.168.1.183	laptoproduccion	laptoproduccion	HCPT_PLAN_G1	00-15-00-36-D1-OA	135	139	445													
122	PC	Producción	192.168.1.184	turismo.hcpt.gov.ec	TURISMO	HCPT_PRO_G1	00-20-A6-58-4E-53	21	25	110													
123	PC	Producción	192.168.1.186	desarrollo4.hcpt.gov.ec	DESARROLLO4	HCPT_PRO_G1	00-20-A6-60-F0-5E	21	25	110	135	139	445										
124	PC	Producción	192.168.1.187	DESARROLLO5	GAMBIENTAL	HCPT_PRO_G1	00-20-A6-58-50-59	21	25	110													
125	PC	Producción	192.168.1.188	PIRT1	PIRT1		00-08-A1-31-65-62	21	25	110	135	139	445										
126	PC	Vias y Construcciones	192.168.1.200	direccionoopp	DIRECCIONOOPP	HCPT_OOPP_G1	00-08-A1-95-04-A4	21	25	110													
127	ACCESS POINT	Vias y Construcciones	192.168.1.201	ORiNOCO-AP-4000M-70-7b-c5	AP-4000M v3.4.0(1146) SN-07UT04560422 v3.1.5	HCPT_OOPP_G1	00-20-A6-70-7B-C5	21	23	25	80	110											
128	PC	Vias y Construcciones	192.168.1.202	secreoopp.hcpt.gov.ec	secreoopp	HCPT_OOPP_G1	00-20-A6-60-82-28	21	25	110													

129	PC	Vias y Construcciones	192.168.1.205	ufvt01.hcpt.gov.ec	ufvt01	HCPT_OOPP_G1	00-20-A6-6F-F2-8E	21	25	110	139	445	
130	PC	Vias y Construcciones	192.168.1.207	ufvt2.hcpt.gov.ec	ufvt3	HCPT_OOPP_G1	00-20-A6-60-82-00	21	25	110			
131	PC	Vias y Construcciones	192.168.1.208	topografoopp.hcpt.gov.ec	topografoopp	HCPT_OOPP_G1	00-20-A6-60-82-D1	21	25	110	135	139	445
132	PC	Vias y Construcciones	192.168.1.210	disenioopp.hcpt.gov.ec	disenioopp	HCPT_OOPP_G1	00-20-A6-60-82-04	21	25	110			
133	PC	Vias y Construcciones	192.168.1.211	jefefiscal.hcpt.gov.ec	jefefiscal		00-19-D1-62-92-AF	21	25	110	135	139	445
134	PC	Vias y Construcciones	192.168.1.212	FISCALOOPP.hcpt.gov.ec	FISCALOOPP	HCPT_OOPP_G1	00-11-11-D4-21-7E	21	25	110	135	139	445
135	PC	Vias y Construcciones	192.168.1.213	Conoopp.hcpt.gov.ec	Conoopp	HCPT_OOPP_G1	00-20-A6-60-F2-B7	21	25	110	135	139	445
136	PC	Vias y Construcciones	192.168.1.214	viasoopp.hcpt.gov.ec	viasoopp	HCPT_OOPP_G1	00-20-A6-60-81-FE	21	25	110	135	139	445
137	PC	Vias y Construcciones	192.168.1.215	jefevias.hcpt.gov.ec	jefevias	HCPT_OOPP_G1	00-20-A6-60-82-D6	21	25	110	135	139	445
138	PC	Vias y Construcciones	192.168.1.216	fiscal2oopp.hcpt.gov.ec	FISCAL2OOPP	HCPT_OOPP_G1	00-20-A6-60-82-22	21	25	110			
139	PC	Vias y Construcciones	192.168.1.217	gisoopp.hcpt.gov.ec	gisoopp	HCPT_OOPP_G1	00-20-A6-60-82-D5	21	25	110	135	139	445
140	PC	Talleres	192.168.1.218	talleres.hcpt.gov.ec	TALLERES	HCPT_OOPP_G1	00-11-11-D4-21-B0	21	25	110			
141	PC	Aula Virtual	192.168.1.220	aulavirtual.hcpt.gov.ec	aulavirtual		00-11-11-A3-F8-C1	21	25	80	110	135	443
142	PC	Gobierno	192.168.1.221	pc01.hcpt.gov.ec	PC01		00-07-E9-E0-2D-5C						
143	PC	Gobierno	192.168.1.222	gente.hcpt.gov.ec	GENTE	HCPT_GOB_G1	00-0D-88-F0-EA-FD						
144	PC	Gobierno	192.168.1.223	escuela.hcpt.gov.ec	ESCUELA		00-07-E9-E0-20-93						
145	PC	Gobierno	192.168.1.224	sociales.hcpt.gov.ec	SOCIALES		00-07-E9-E0-17-4A						
146	PC	Gobierno	192.168.1.225	trabajo.hcpt.gov.ec	TRABAJO	HCPT_GOB_G1	00-12-17-8A-8F-00						
147	PC	Gobierno	192.168.1.226	agua2.hcpt.gov.ec	AGUA2		00-08-54-09-08-4B						
148	PC	Gobierno	192.168.1.227	biblio001.hcpt.gov.ec	BIBLIO001		00-16-17-C9-E2-08						
149	ACCESS POINT	Gobierno	192.168.1.229	Linksys WAP54G		HCPT_GOB_G1	00-90-4C-91-00-01						
150	SWITCH	Sistemas	192.168.1.250	3COM 4226T 1 HCPT			00-0E-6A-F6-27-60	21	25	110			
151	SWITCH	Sistemas	192.168.1.251	3COM 4226T 2 HCPT			00-0F-CB-71-BB-20	21	23	25	80	110	
152	SWITCH	Sistemas	192.168.1.252	3COM 3300XM 1 HCPT			00-0A-04-61-B6-98	21	23	25	80	110	
153	SWITCH	Sistemas	192.168.1.253	3COM 3300XM 2 HCPT			00-0A-04-5F-7A-F8	21	23	25	80	110	

Anexo 2: Vista satelital de las infraestructuras Físicas del H. Consejo Provincial de Tungurahua

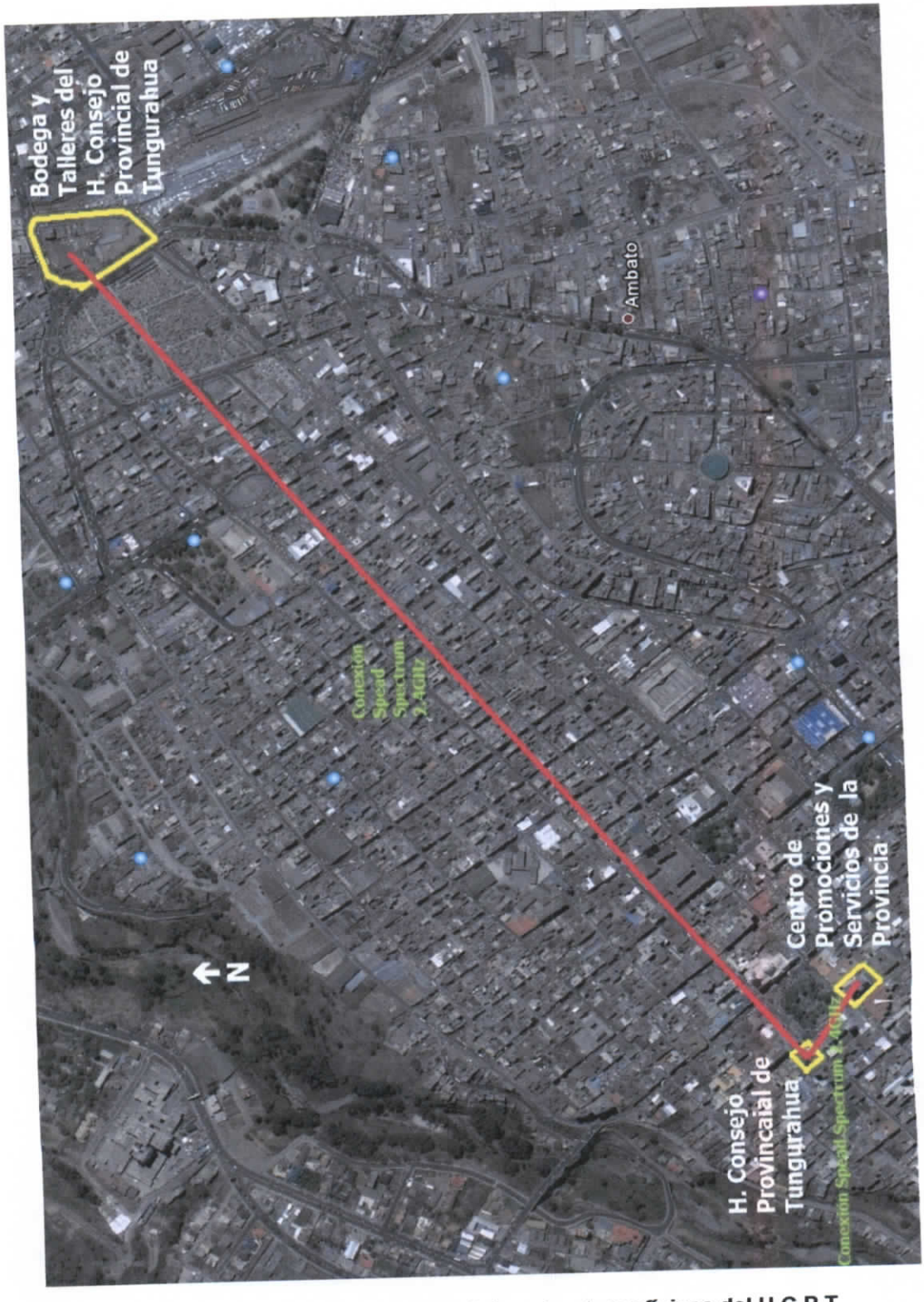


Figura 102: Vista Satelital de las Infraestructuras físicas del H.C.P.T.

Anexo 3: Dispositivos de comunicación Inalámbrica, Access Point Orinoco

Figura 103: Access Point Oricono AP-4000

Anexo 4: Antenas de Spead Spectrum para la comunicación remota en la terraza del H.C.P.T.

Figura 104: Antenas Spread Spectrum del H. Consejo Provincial de Tungurahua

Anexo 5: Antenas de Spread Spectrum en la Terraza del Edifcio del Centro de Promociones y servicios de la Provincia

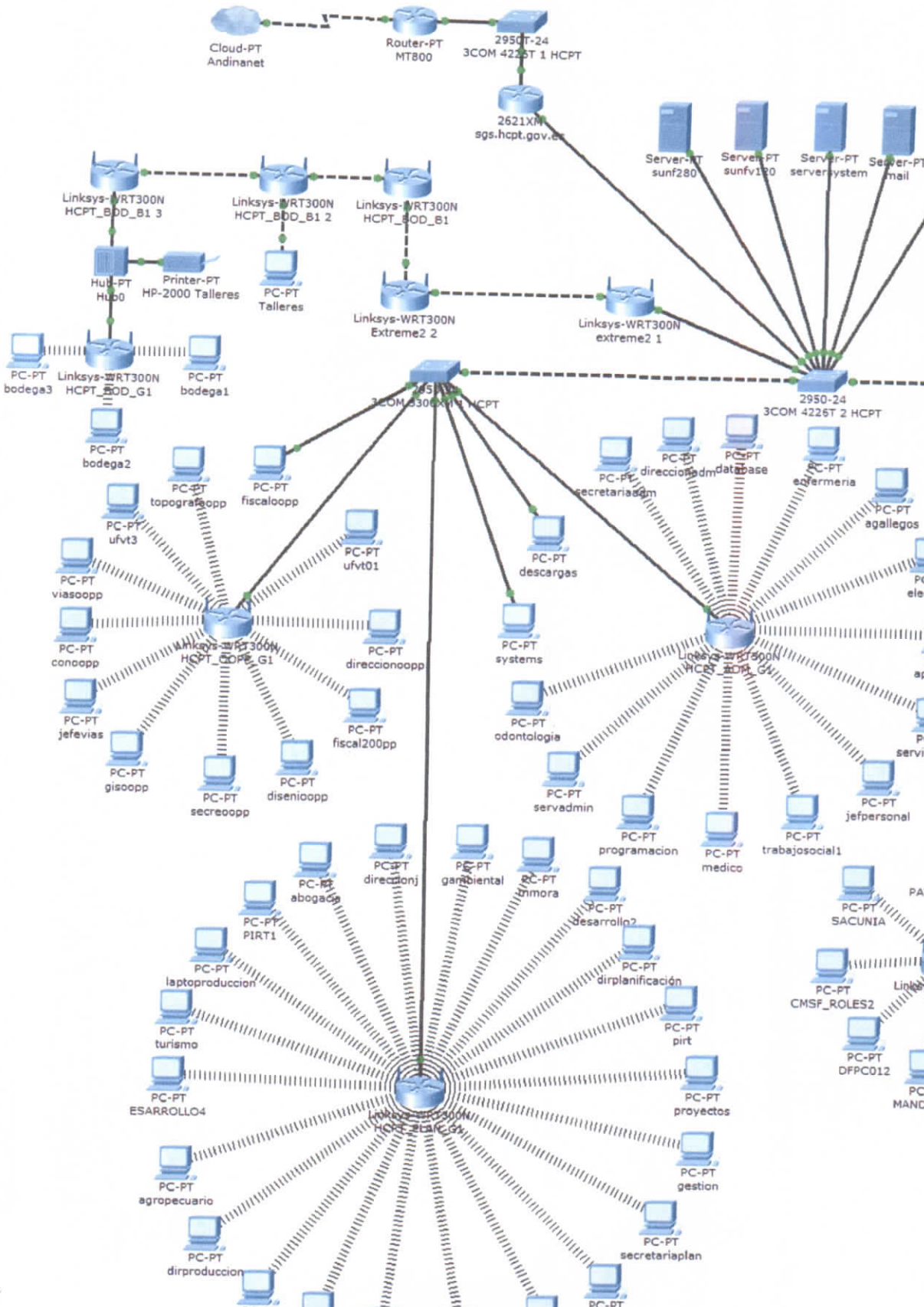
Figura 105: Antena Spread Spectrum del Gobierno Provincial

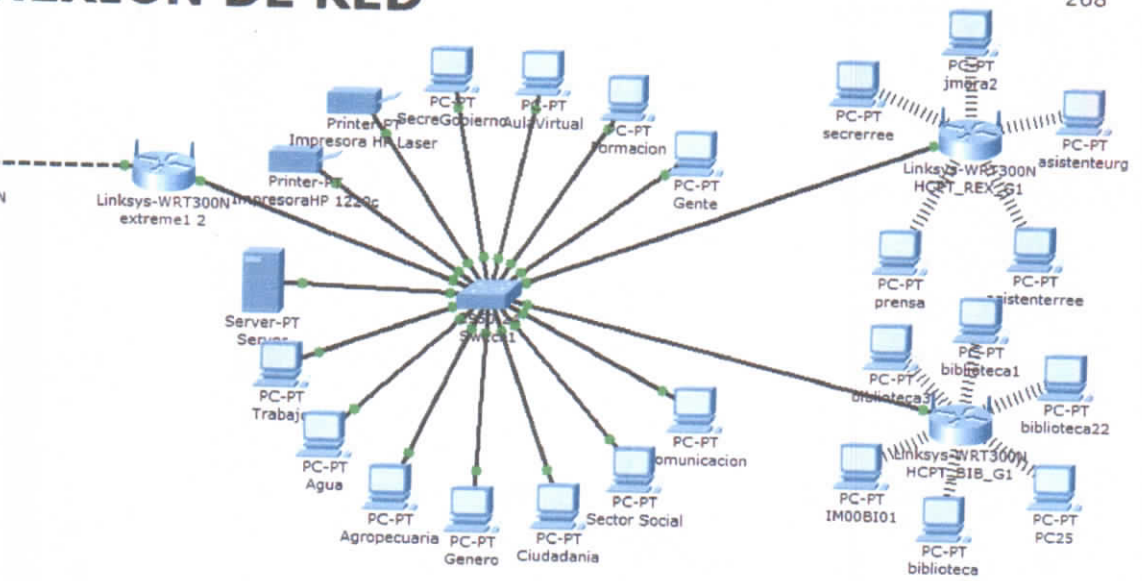
Anexo 6: Antenas de Spread Spectrum para el área de talleres y bodega, estas antenas están ubicadas en la Terraza del Edificio del Sindicato de Trabajadores del H. Consejo Provincial de Tungurahua,

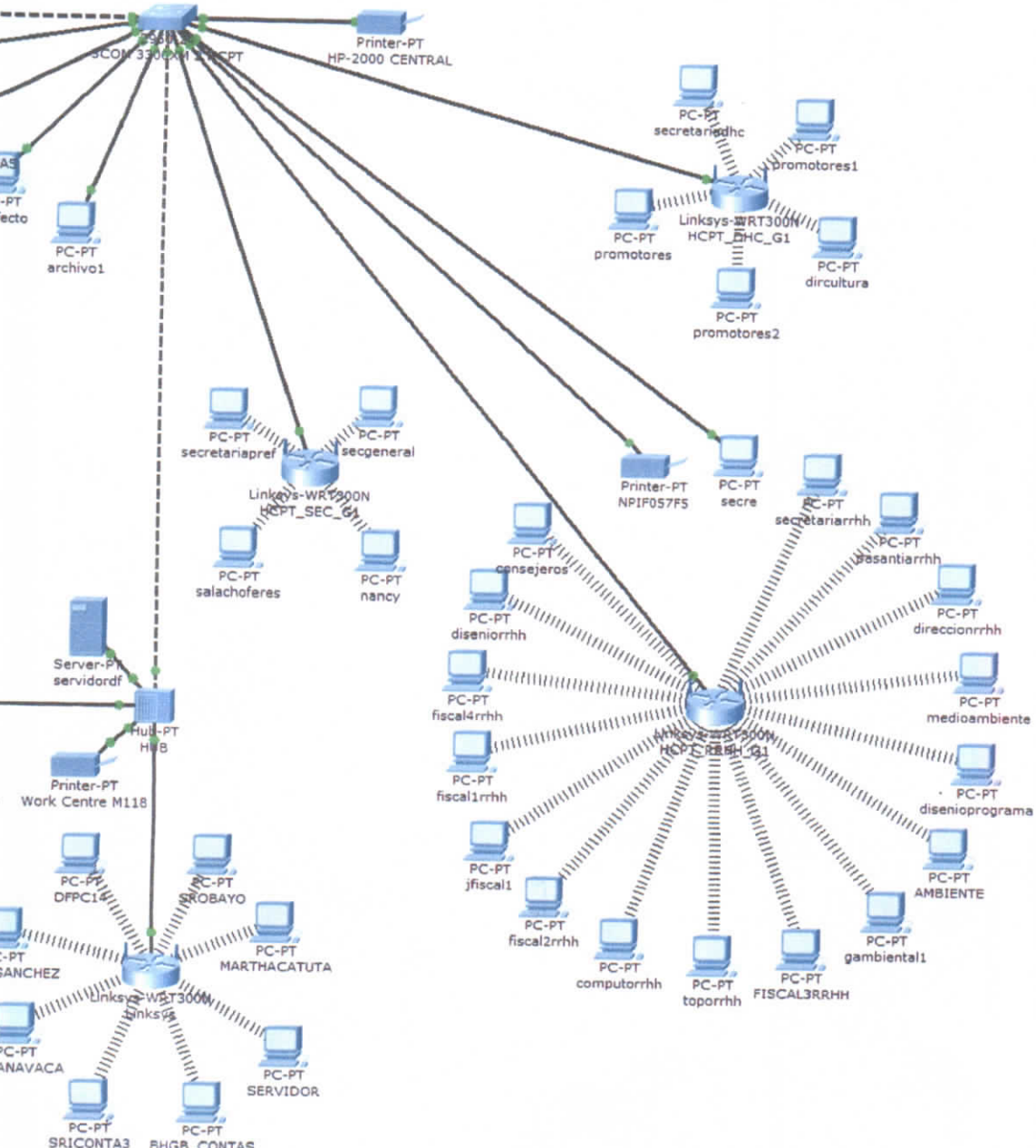
Figura 106: Antenas Spread Spectrum de Bodega y Talleres del HCPT

Anexo7:

H. CONSEJO PRO
ESQUEMA DE I




Linksys-WRT300N
extreme1 2
Printer-PT
Impresora HP Laser
Printer-PT
ImpresoraHP 1220c
PC-PT
SecreGobierno
PC-PT
AulaVirtual
PC-PT
formacion
PC-PT
Gente
Server-PT
Server
PC-PT
Trabaj
PC-PT
Agua
PC-PT
Agropecuaria
PC-PT
Genero
PC-PT
Ciudadania
PC-PT
Sector Social
PC-PT
omunicacion
PC-PT
jmora2
PC-PT
secrerree
Linksys-WRT300N
HCPT_REX_G1
PC-PT
asistenteurg
PC-PT
prensa
PC-PT
PC-PT
biblioteca1
PC-PT
biblioteca22
Linksys-WRT300N
HCPT_BIB_G1
PC-PT
IM00BI01
PC-PT
biblioteca
PC-PT
PC25


Printer-PT
HP-2000 CENTRAL
PC-PT
archivo1
PC-PT
secretariadhc
PC-PT
promotores1
Linksys-WRT300N
HCPT_DHC_G1
PC-PT
promotores
PC-PT
dircultura
PC-PT
promotores2
PC-PT
secretariapref
PC-PT
secgeneral
Linksys-WRT300N
HCPT_SEC_G1
PC-PT
salachoferes
PC-PT
nancy
Printer-PT
NPIF057F5
PC-PT
secre
PC-PT
secretariarrhh
PC-PT
asantiarrhh
PC-PT
direccionrrhh
PC-PT
consejeros
PC-PT
diseniorrhh
PC-PT
fiscal4rrhh
PC-PT
fiscal1rrhh
PC-PT
medioambiente
PC-PT
diseniopograma
PC-PT
AMBIENTE
PC-PT
gambiental1
PC-PT
jfiscal1
PC-PT
fiscal2rrhh
PC-PT
computorrhh
PC-PT
toporrhh
PC-PT
FISCAL3RRHH
Server-PT
servidordf
Hub-PT
HUB
Printer-PT
Work Centre M118
PC-PT
DFPC14
PC-PT
ROBAYO
PC-PT
MARTHACATUTA
PC-PT
SERVIDOR
PC-PT
SRICONTA3