



UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIA Y TECNOLOGÍA

ESCUELA DE INGENIERÍA ELECTRÓNICA

**Diseño de una red multiservicios basados en tecnología NGN
para el Centro de Alto Rendimiento de la ciudad de Cuenca**

**Trabajo de graduación previo a la obtención del título de
Ingeniero Electrónico**

AUTOR:

JUMBO SOTO WILMER FERNANDO

DIRECTOR:

PÉREZ RODRÍGUEZ LEONEL

Cuenca- Ecuador

2011

DEDICATORIA

Dedico este trabajo a mi familia, en especial a mis padres que siempre estuvieron a mi lado a cada momento brindándome su apoyo y cariño para poder concluir esta etapa tan importante de mi vida.

Wilmer Fernando Jumbo Soto.

AGRADECIMIENTOS

Agradezco de manera especial a las personas que formaron parte de toda mi carrera estudiantil, al personal docente de la Universidad del Azuay que ciclo tras ciclo me brindaron sus conocimientos para llegar a esta etapa en la vida de profesional, al ingeniero Leonel Pérez por su ayuda en la corrección y guía del presente trabajo monográfico, a mis compañeros y amigos que siempre estuvieron a mi lado brindándome su amistad, apoyo y ayuda, a mi familia que fue el pilar fundamental para seguir siempre adelante.

RESUMEN

Para el diseño de una red multiservicio, se calcula mediante estimaciones y fórmulas un ancho de banda de internet; los sistemas de voz, datos, videovigilancia y sistemas contra incendios fueron diseñados en una misma plataforma de red con protocolo IP porque pueden converger mediante la colocación de los mismos en redes VLAN que separarían de manera lógica estos sistemas, los mismos que están programados en equipos CISCO de alta tecnología permitiendo al administrador de red el control total de estos sistemas, con la finalidad de evitar deficiencias, brindar una buena calidad de servicio y para dar al usuario final la comodidad que este necesita.

PALABRAS CLAVE:

- **UIT** Unión Internacional de Telecomunicaciones.
- **VoIP.** Voz sobre IP.
- **LAN.** Red de Área Local.
- **VLAN.** Red de Área Local Virtual.
- **PSTN.** Red Telefónica Pública Conmutada.
- **PoE.** Energía a través de Ethernet.
- **SIP.** Protocolo de Inicio de Sesión.
- **QoS.** Calidad de Servicio.
- **IP.** Protocolo de Internet

ABSTRACT

In order to design a multiservice network, we calculate through estimates and formulations an internet broadband; in addition, voice, data, video vigilance, and fire systems were designed in a same net platform with IP protocol because they might converge by the setting of them in VLAN networks which they would separate in a logic manner these systems. They are also programmed under high-technology CISCO equipment allowing the network administrator a full control from the systems with the purpose to avoid difficulties, to give a quality of service, and to give a comfort that the final user needs.

KEYWORDS:

- **ITU** International Telecommunications Union.
- **VoIP.** Voice Over IP.
- **LAN.** Local Area Network.
- **VLAN.** Virtual Local Area Network.
- **PSTN.** Public Switched Telephone Network.
- **PoE.** Power Over Ethernet.
- **SIP.** Session Initiation Protocol.
- **QoS.** Quality of Service.
- **IP.** Internet Procol

INDICE DE CONTENIDOS

DEDICATORIA	ii
AGRADECIMIENTO.....	iii
RESUMEN	iv
ABSTRACT	v
INDICE DE CONTENIDOS	vi
INDICE DE ANEXOS	viii
INDICE DE FIGURAS	ix
INDICE DE TABLAS.....	x
 INTRODUCCIÓN	 1

CAPÍTULO 1: CONCEPTOS PRINCIPALES

1.1. Redes Multiservicio.	2
1.2. Redes de Nueva Generación (NGN).....	3
1.2.1. Definición y características de las redes NGN.....	3
1.2.2. Arquitectura de una red NGN	4
1.3. Aplicaciones Basadas en NGN.	5
1.3.1. VoIP (Voz sobre IP).	5
1.3.1.1. Ventajas de VoIP.....	6
1.3.1.2. Tecnologías VoIP.	6
1.3.1.3. Elementos implicados en VoIP.....	7
1.3.1.4. Funcionamiento General de un sistema VoIP con protocolo SIP... 8	
1.3.2. VideoVigilancia IP.	10
1.3.2.1. Sistemas de Videovigilancia.	10
1.3.2.2. Diferencias entre CCTV (analógico) y Videovigilancia IP.....	13
1.3.3. Seguridad Contra incendios.	13
1.3.3.1. Elementos que intervienen en un sistema contra incendios.	15

CAPÍTULO 2: REQUERIMIENTOS DE LA RED

2.1.	Requerimiento de aplicaciones y puntos de red de la planta baja.....	17
2.2.	Requerimiento de aplicaciones y puntos de red de la primera planta	18
2.3.	Requerimiento de aplicaciones y puntos de red de la segunda planta.....	20
2.4.	Requerimiento de aplicaciones y puntos de red de la tercera planta.	22
2.5.	Requerimiento de aplicaciones y puntos de red de cuarta y quinta planta....	23
2.6.	Requerimientos totales de aplicaciones y puertos de red	26
2.7.	Cálculo estimado de ancho de banda de internet	26
2.8.	Cuartos de telecomunicaciones	28
2.9.	Equipos a Utilizarse en el diseño de red	29
2.9.1.	Router Cisco Serie 2800.....	29
2.9.2.	Switches de la serie cisco Catalyst 2960.....	30
2.9.3.	Cámara IP cisco PVC2300	32
2.9.4.	Teléfono IP Cisco 7960.....	33
2.9.5.	Cisco MCS 7816-I4.....	34
2.9.5.1.	Cisco Unified Communications Manager.....	34
2.9.6.	Puntos de acceso inalámbricos Cisco WAP2000	35
2.9.7.	Paneles de alarma contra incendios Vista32FB de Honeywell	37
2.9.7.1.	Comunicador IP Avatec IPCOM4	39

CAPÍTULO 3: DISEÑO DE LA RED MULTISERVICIO

3.1.	Consideraciones para el diseño de red.	40
3.2.	Redes VLAN.....	40
3.2.1.	Beneficios de una VLAN.....	41
3.3.	Diseño de las redes VLAN	49
3.3.1.	Asignación de VLANs por Departamento	49
3.4.	Funcionamiento y configuración de los equipos de red.....	49
3.5.	Costo de equipos a utilizarse en el diseño de red	56
CONCLUSIONES.		57
RECOMENDACIONES.		58
BIBLIOGRAFÍA		59
ANEXOS.		61

ÍNDICE DE ANEXOS

ANEXO 1: Distribución VLAN 10: Almacenes.....	61
ANEXO 2: Distribución VLAN 20: VLAN AP	61
ANEXO 3: Distribución VLAN 30: VLAN Administración	62
ANEXO 4: Distribución VLAN 40: VLAN Alarmas.....	62
ANEXO 5: Distribución VLAN 50: VLAN Voz.....	63
ANEXO 6: Distribución VLAN 60: VLAN Videovigilancia.....	65
ANEXO 7: Distribución VLAN 70: VLAN Videovigilancia.....	65
ANEXO 8: Diseño de la red multiservicio de la planta baja	66
ANEXO 9: Diseño de la red multiservicio de la primera planta.....	66
ANEXO 10: Diseño de la red multiservicio de la segunda planta	66
ANEXO 11: Diseño de la red multiservicio de la tercera planta.....	66
ANEXO 12: Diseño de la red multiservicio de la cuarta planta.....	66
ANEXO 13: Diseño de la red multiservicio de la quinta planta	66
ANEXO 14: Diagrama vertical de la red multiservicio.....	66

ÍNDICE DE FIGURAS

Fig. 1.1. Comparación Redes clásicas vs Redes de Nueva Generación.	4
Fig. 1.2. Teléfonos IP Cisco.....	7
Fig. 1.3. Adaptador analógico.....	7
Fig. 1.4. Softphones	8
Fig. 1.5. Centralillas IP	8
Fig. 1.6. Ejemplo de establecimiento de llamada	9
Fig. 1.7. Esquema de videovigilancia analógica.....	10
Fig. 1.8. Esquema de videovigilancia analógica con DVR	11
Fig. 1.9. Esquema de videovigilancia con servidor de video	11
Fig. 1.10. Esquema de videovigilancia IP	11
Fig. 1.11. Cámaras de red fijas con versiones inalámbricas y megapíxel.	12
Fig. 1.12. Cámaras de red domo fijas	12
Fig. 1.13. Cámaras de red domo PTZ	12
Fig. 1.14. Funcionamiento de un sistema de alarmas convencional	14
Fig. 1.15. Funcionamiento de un sistema de alarmas direccionable.....	14
Fig. 1.16. Configuración de equipos para alarma contra incendios.....	15
Fig. 1.17. Panel de Alarma Honeywell Silent Knight.	16
Fig. 1.18. Detector de Humo fotoeléctrico	16
Fig. 1.19. Principio de funcionamiento de sensores de humo	16
Fig. 2.1. Topología de red general de la planta baja.....	18
Fig. 2.2. Topología de red general de la primera planta	19
Fig. 2.3. Topología de red general de la segunda planta (A)	20
Fig. 2.4. Topología de red general de la segunda planta (B).....	21
Fig. 2.5. Topología de red general de la tercera planta (A).....	22
Fig. 2.6. Topología de red general de la tercera planta (B)	23
Fig. 2.7. Topología de red general de la cuarta y quinta planta (A)	24
Fig. 2.8. Topología de red general de la cuarta y quinta planta (B)	25
Fig. 2.9. Disposición de los cuartos de comunicaciones	29
Fig. 2.10. Cisco Router 2800 series	29
Fig. 2.11. Cisco Switch Catalyst 2960	30
Fig. 2.12. Cámara IP Cisco PVC2300	32
Fig. 2.13. Teléfono IP Cisco 7960.....	33
Fig. 2.14. AP Cisco WAP2000.....	35
Fig. 2.15. Panel de alarma Vista 32FB Honeywell	37
Fig. 2.16. IPCOM4	39
Fig. 3.1. Beneficios de una red VLAN	41

INDICE DE TABLAS

Tabla 1.1: Comparativa de códecs.....	7
Tabla 1.2: Diferencias entre CCTV analógica y videovigilancia IP	13
Tabla 2.1: Número de aplicaciones y puntos de red de la planta baja	17
Tabla 2.1.1: Cámaras IP a utilizarse en la planta baja.....	18
Tabla 2.2: Número de aplicaciones y puntos de red de la primera planta.....	19
Tabla 2.2.1: Cámaras IP a utilizarse en la primera planta.	19
Tabla 2.3: Número de aplicaciones y puntos de red de la segunda planta (A).....	20
Tabla 2.3.1: Cámaras IP a utilizarse en la segunda planta (A).....	20
Tabla 2.3.2: Número de aplicaciones y puntos de red de la segunda planta (B).....	21
Tabla 2.3.3: Cámaras IP a utilizarse en la segunda planta (B).....	21
Tabla 2.4: Número de aplicaciones y puntos de red de la tercera planta (A)	22
Tabla 2.4.1: Cámaras IP a utilizarse en la tercera planta (A).	22
Tabla 2.4.2: Número de aplicaciones y puntos de red de la tercera planta (B)	23
Tabla 2.4.3: Cámaras IP a utilizarse en la tercera planta (B).	23
Tabla 2.5: Número de aplicaciones y puntos de red de la cuarta y quinta planta (A).....	24
Tabla 2.5.1: Cámaras IP a utilizarse en la cuarta y quinta planta (A).	24
Tabla 2.5.2: Número de aplicaciones y puntos de red de la cuarta y quinta planta (B)...	25
Tabla 2.5.3: Cámaras IP a utilizarse en la cuarta y quinta planta (B).	25
Tabla 2.6: Total de puertos y aplicaciones del edificio	26
Tabla 2.7: Distribución estimada de usuarios por planta	26
Tabla 2.8. Datos Técnicos MCS Cisco 7816-I4.	34
Tabla 2.9. Datos Técnicos AP WAP 2000.....	36
Tabla 3.1. Especificación del sistema de datos de la planta baja.....	42
Tabla 3.1.1. Especificación del sistema de datos de la primera planta	43
Tabla 3.1.2a Especificación del sistema de datos de la segunda planta (A).	43
Tabla 3.1.2b Especificación del sistema de datos de la segunda planta (B)	44
Tabla 3.1.3a Especificación del sistema de datos de la tercera planta (A).....	44
Tabla 3.1.3b Especificación del sistema de datos de la tercera planta (B).....	44
Tabla 3.1.4a Especificación del sistema de datos de la cuarta y quinta planta (A)	45
Tabla 3.1.4b Especificación del sistema de datos de la cuarta y quinta planta (B).	45
Tabla 3.1.5. Distribución de interfaces de switches de la planta baja.....	46
Tabla 3.1.6. Distribución de interfaces de switches de la primera planta	46
Tabla 3.1.7. Distribución de interfaces de switches de la segunda planta (A)	47
Tabla 3.1.8. Distribución de interfaces de switches de la segunda planta (B)	47
Tabla 3.1.9. Distribución de interfaces de switches de la tercera planta (A).....	48
Tabla 3.1.10. Distribución de interfaces de switches de la tercera planta (B).....	48

Tabla 3.1.11. Distribución de interfaces de switches de la cuarta y quinta planta (A)	48
Tabla 3.1.12. Distribución de interfaces de switches de la cuarta y quinta planta (B)	48
Tabla 3.2. Tabla de calidad y ancho de banda cámara PVC2300	51
Tabla 3.3. Servicios disponibles en comunicador IP de Avatec	52
Tabla 3.4. Costo de equipos para la Implementación del diseño de red	56

[Red handwritten signature]
31/10/11

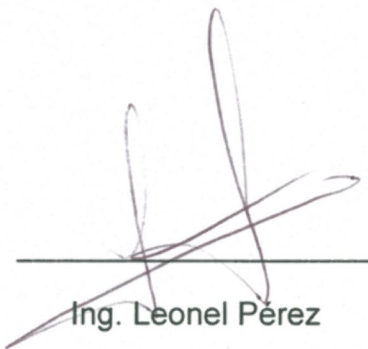
DISEÑO DE UNA RED MULTISERVICIOS BASADOS EN TECNOLOGÍA NGN PARA EL CENTRO DE ALTO RENDIMIENTO DE LA CIUDAD DE CUENCA

RESUMEN

Para el diseño de una red multiservicio, se calcula mediante estimaciones y fórmulas un ancho de banda de internet; los sistemas de voz, datos, videovigilancia y sistemas contra incendios fueron diseñados en una misma plataforma de red con protocolo IP porque pueden converger mediante la colocación de los mismos en redes VLAN que separarían de manera lógica estos sistemas, los mismos que están programados en equipos CISCO de alta tecnología permitiendo al administrador de red el control total de estos sistemas, con la finalidad de evitar deficiencias, brindar una buena calidad de servicio y para dar al usuario final la comodidad que este necesita.



Fernando Jumbo



Ing. Leonel Pérez

Handwritten in red: 31/10/11

**DESIGN OF A MULTISERVICES NETWORK BASED ON NGN
TECHNOLOGY FOR THE CUENCA'S HIGH PERFORMANCE CENTER**

ABSTRACT

In order to design a multiservice network, we calculate through estimates and formulations an internet broadband; in addition, voice, data, video vigilance, and fire systems were designed in a same net platform with IP protocol because they might converge by the setting of them in VLAN networks which they would separate in a logic manner these systems. They are also programmed under high-technology CISCO equipment allowing the network administrator a full control from the systems with the purpose to avoid difficulties, to give a quality of service, and to give a comfort that the final user needs.



Fernando Jumbo



Ing. Leonel Pérez

Jumbo Soto Wilmer Fernando
Trabajo de Graduación
Ing. Leonel Pérez
Noviembre del 2011

DISEÑO DE UNA RED MULTISERVICIOS BASADOS EN TECNOLOGÍA NGN PARA EL CENTRO DE ALTO RENDIMIENTO DE LA CIUDAD DE CUENCA

INTRODUCCIÓN

Con el creciente desarrollo y avance de la tecnología en las telecomunicaciones, las redes NGN (*New Generation Network*) son las redes mas opcionadas para las futuras edificaciones que deberán incluir soluciones de última tecnología en su interior para brindar servicios de voz, datos y video dentro de una misma plataforma de red, además de redes de vigilancia y seguridad con el fin de concebir una edificación moderna y eficaz.

Actualmente muy pocas empresas cuentan con un sistema de integración de servicios que les facilite la administración de los mismos evitando así sistemas ineficientes y baja calidad en los servicios. Por otra parte los sistemas de seguridad y de vigilancia son tratados independientemente de los servicios de voz y datos, resultando la administración de los mismos más compleja y con un costo de mantenimiento elevado.

El centro de alto rendimiento que debía inaugurarse en el año 2008 no ha sido inaugurado por falta de finalización en todos sus contratos por lo que no cuenta aún con una red avanzada y con una alta tendencia al crecimiento como sucede en las redes multiservicio. La red NGN al ser basada en el protocolo IP depende de una dirección IP para que múltiples equipos se comuniquen sin problemas y tengan una alta tendencia de escalabilidad.

La integración de estos servicios en una sola plataforma resulta ser una solución que aprovecha los beneficios de equipos de última tecnología en voz, datos, vigilancia y seguridad, equipos que manejan actualmente protocolos de internet que sistemas convencionales no soportan. La implementación de una red multiservicio moderna de este tipo resulta eficaz para este centro que albergará visitas de deportistas a nivel internacional los cuales requerirán servicios de comunicaciones sin problemas de ineficiencia y comodidad.

CAPÍTULO I

CONCEPTOS PRINCIPALES

1.1 Redes Multiservicio.

Las redes multiservicio resultan muy beneficiosas para empresas proveedoras de servicios de telecomunicaciones debido a la excelente relación entre costos, comodidad y facilidad de administración y mantenimiento. Las operadoras de redes de telecomunicaciones continúan actualmente ofreciendo servicios de manera independiente, o sea, servicios administrados por separado que llevan la información a través de enlaces troncales de alta velocidad de tipo *Optical Carrier (OC)*, como, por ejemplo el OC-48, que soporta una tasa de transferencia de 2488.32 Mbit/s.

Sin embargo, con el crecimiento de la tecnología cada vez las demandas por parte de usuarios crece, los servicios multimedia se hacen cada vez más presentes en la vida cotidiana de los usuarios; debido a esto las grandes empresas de telecomunicaciones se ven obligados a competir con otras empresas migrando a una infraestructura de red moderna y con gran tendencia al crecimiento y la integración de servicios.

Un ejemplo claro de competencia en la ciudad es la operadora de cable TVCABLE que compite con los operadores tradicionales en el negocio de acceso a Internet de banda ancha, tanto para clientes residenciales como corporativos. Como respuesta a retos de demanda de ancho de banda, calidad de servicios (QoS) los operadores están implementando redes de próxima generación que estarán en capacidad de adaptarse a cualquier dispositivo que tenga acceso al protocolo IP, es decir, cuando un usuario conecte el dispositivo, la red será capaz de adaptarse a él en función de sus necesidades de ancho de banda. Para ello, la red debe evitar las diferencias existentes entre las aplicaciones CBR (*Constant-Bit-Rate*), como la voz, y las aplicaciones VBR (*Variable-Bit-Rate*), como los datos.

Los beneficios principales de una red multiservicio de nueva generación son los siguientes:

- Optimiza el uso de los medios.
- Reduce los costos asociados a la renta de los medios.
- Simplifica la administración de la infraestructura.
- Reduce los costos de operación de la red.

Los beneficios de una red multiservicio dentro de un edificio significan un ahorro importante

para la empresa, ya que simplifican los costos de mantenimiento, costos de administración de la red, facilitan el monitoreo por parte del personal de TI (gente especializada en Tecnologías de Información) y son capaces de brindar un mejor servicio para los usuarios de la empresa.

1.2 Redes de Nueva Generación NGN.

1.2.1 Definición y características de las redes de nueva generación.

De las numerosas definiciones de NGN, se destaca la definición dada por el Sector de Normalización de la Unión Internacional de Telecomunicaciones (UIT – T) dada en la Recomendación Y.2001, que define a una red NGN como: *“Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios”*.

Según la Recomendación Y.2001 las características principales de una red NGN son:

- La transferencia estará basada en paquetes.
- Las funciones de control están separadas de las capacidades de portador, llamada/sesión, y aplicación/servicio.
- Desacoplamiento de la provisión del servicio del transporte, y se proveen interfaces abiertas.
- Soporte de una amplia gama de servicios, aplicaciones y mecanismos basados en construcción de servicios por bloques (incluidos servicios en tiempo real/de flujo continuo en tiempo no real y multimedia).
- Tendrá capacidades de banda ancha con calidad de servicio (QoS) extremo a extremo.
- Tendrá interoperabilidad con redes tradicionales a través de interfaces abiertas.
- Movilidad generalizada.
- Acceso sin restricciones de los usuarios a diferentes proveedores de servicios.
- Características unificadas para el mismo servicio, como es percibida por el usuario.
- Convergencia entre servicios fijos y móviles.
- Independencia de las funciones relativas al servicio con respecto a las tecnologías subyacentes de transporte.
- Soporte de las múltiples tecnologías de última milla.
- Cumplimiento de todos los requisitos reglamentarios, por ejemplo, en cuanto a comunicaciones de emergencia, seguridad, privacidad, interceptación legal, etc.

(Rec. UIT-T)

La tecnología NGN (*New Generation Network*) llega a desarrollarse sobre una plataforma conocida como IMS (*International Protocol Multimedia System*), la cual permite la convergencia de servicios de datos, video y multimedia. El dibujo de la figura 1.1 representa una comparación de la gestión e infraestructura de las redes clásicas con las redes de nueva generación. Se observa que en las redes clásicas los servicios y gestión de los mismos se basan en un sistema vertical e independiente y en redes de nueva generación, todo lo contrario: una convergencia total.

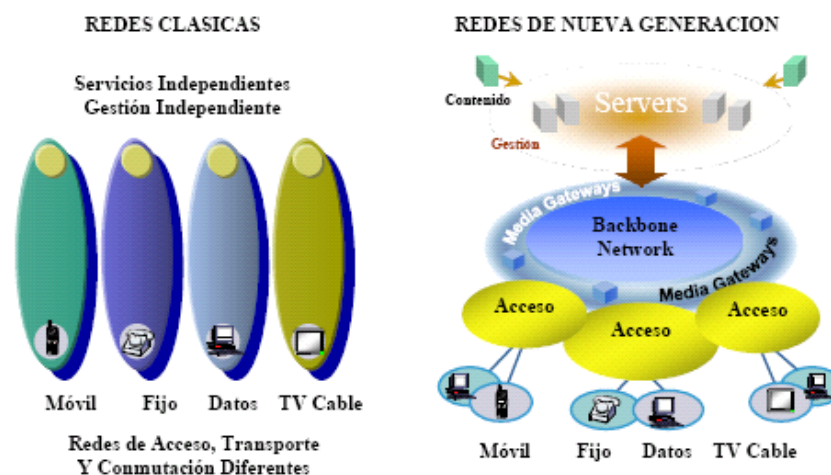


Fig.1.1 Comparación Redes clásicas vs. Redes de Nueva Generación (Fuente: Módulo Redes de Nueva Generación: Documento de lectura 1 Ing. Diego Uribe)

1.2.2 Arquitectura de una red NGN

Las redes NGN requieren una arquitectura que permita la integración de servicios de telecomunicaciones nuevos y tradicionales, esta arquitectura está conformada por 4 capas principales: conectividad, acceso, servicio y gestión.

- **Capa de Conectividad Primaria y Transporte.-** En esta capa el tráfico se transporta de extremo a extremo usando una red IP. Siempre se deberá garantizar la calidad de servicio (QoS) ya que el tráfico de los clientes no debe ser afectado por perturbaciones de la calidad, tales como retardos, fluctuaciones y ecos. Esta capa está constituida por un *Gateway* cuya función es adaptar el tráfico del cliente y de control a la tecnología de la NGN. Los *Gateways* se interconectan con otras redes, en cuyo caso son llamados *gateways* de red, o directamente con los equipos de usuarios finales denominados *gateways* de acceso.
- **Capa de Acceso.-** Provee el acceso a los servicios de la red NGN independiente del tipo de terminal y medio empleado. El *gateway* de acceso provee la conversión necesaria de la información de la fuente a IP y viceversa, actuando bajo el mando del controlador de llamadas de la capa de servicio.

La capa de acceso incluye las diversas tecnologías usadas para llegar a los clientes. Los sistemas de cable, xDSL e inalámbricos como wifi o wimax se cuentan entre las soluciones más prometedoras que están creciendo e introduciendo innovaciones rápidamente.

- **Capa de Servicio.-** Esta capa consiste de los equipos que proporcionan los servicios y aplicaciones disponibles para la red. Los servicios se ofrecen para toda la red, sin que importe la ubicación del usuario siendo tan independientes como sea posible de la tecnología de acceso que se use. Esta capa hace posible distribuir los servicios hacia los equipos de los usuarios finales, en vez de distribuirlos en la red. Los tipos de servicios que se ofrecerán abarcarán todos los existentes para voz, datos y nuevos servicios multimedia.
- **Capa de Gestión.-** Como su nombre indica, es la capa donde se controlan los diferentes tipos de sesiones entre los terminales y los *gateways*. Garantiza el soporte, supervisión, recuperación y análisis del desempeño de la red. La eficiencia de esta capa depende de la cantidad y tipos de servicios brindados.

1.3 Aplicaciones basadas en NGN

1.3.1 VoIP (Voz sobre IP)

La Voz sobre IP (*Internet Protocol*) es la tecnología que permite la transmisión de señales de voz a través de Internet.

La comunicación telefónica tradicional consistía en la conmutación de circuitos que implicaba la apertura de un canal permanentemente lo cual representaba un alto consumo de los recursos de la red de telefonía convencional, además de correr muchos riesgos de interferencia o el denominado *crosstalk*. Con el fin de reemplazar este tipo de tecnología nace la voz sobre IP basada en la digitalización de la voz y el envío de la misma mediante tramas IP.

La VoIP llega a extenderse al punto de poder realizar llamadas desde los mismos PCs mediante la instalación de softwares denominados *Softphones* que emulan el funcionamiento de un equipo telefónico real. El principal servicio de los diferentes proveedores de Voz sobre IP es el de hacer de pasarela hacia la red telefónica pública (conocida como PSTN/POTS) a costos muy reducidos, un ejemplo de estos puede ser el proveedor de VoIP conocido como Skype.

1.3.1.1 Ventajas de VoIP

Las principales ventajas de VoIP se pueden resumir en las siguientes:

- Reduce los gastos tanto de equipos como costos por el servicio.
- Tener un número de teléfono que suena a la vez en varios dispositivos, para ayudar a sus empleados a estar conectados entre sí y con sus clientes.
- Utilizar una sola red para voz y datos, simplificando la gestión y reduciendo costos.
- Acceder a las funciones de su sistema telefónico en casa o bien en las oficinas de sus clientes, en aeropuertos, hoteles o en cualquier parte donde haya una conexión de banda ancha.

1.3.1.2 Tecnologías Voz sobre IP.

En un sistema VoIP se requieren ciertos protocolos de comunicación que sirven para el establecimiento de las comunicaciones de voz, algunos protocolos serán gestionados desde los dispositivos que se utilicen. En el caso de sistemas CISCO estos protocolos son administrados desde el software denominado *Cisco Call Manager*. A continuación se presentan los protocolos más comunes que se utilizan en VoIP:

- **Protocolo IAX2** .- Protocolo exclusivo de Asterisk que usa el puerto 4569 UDP
- **Protocolo H.323**.- Es un protocolo recomendación de la UIT que provee especificaciones para ordenadores y equipos que se usen dentro de la sesión, es un protocolo no fiable en el caso de video y voz, por lo cual es usado en sistemas en los que no se requiere mayores garantías en calidad de servicio.
- **SIP (Protocolo de Inicio de Sesión)**.- Es el protocolo encargado de iniciar una sesión para la comunicación de los dispositivos del sistema VoIP, trabaja junto con el protocolo SDP que es el encargado de identificar el contenido que tendrá la sesión multimedia y con el protocolo RTP (*Real-time Transport Protocol*) el cual lleva los contenidos de voz o vídeo dentro de la sesión realizada por SIP.

En VoIP, la voz tiene que ser digitalizada para su envío por la red, este procedimiento se hace mediante códecs como G.711, G729A, GSM, iLBC, Speex, G.723. Los dispositivos que conforman un sistema VoIP soportan distintos tipos de códecs que al comunicarse entre ellos negocian un códec en común para el establecimiento de llamada.

A continuación en la Tabla 1.1 se muestra las características de los códecs más usados en VoIP

Tabla 1.1 Comparativa de Códecs (Fuente: Curso voz sobre IP y asterisk v1.0. Módulo I)

Tecnologías Voz sobre IP: Comparativa de Codecs			
CODEC	Codec Bitrate	Intervalo	A. Banda(Ethernet)
G.711	64 Kbps	10ms	87 Kbps
G.729	8 Kbps	10ms	31,2 Kbps
Speex	4-44,2 Kbps	30	17,63 - 59,63 Kbps
ILBC	13,3 Kbps	30	30,83 Kbps
G.723.1	6,3 Kbps	37	21,9 Kbps
GMS	13,2 Kbps	20	28,63 Kbps

1.3.1.3. Elementos implicados en Telefonía IP.

- **Teléfonos IP:** Teléfonos destinados exclusivamente para sistemas VoIP, cuentan con un puerto RJ45 para la conexión de un cable Ethernet; los teléfonos tipo cisco cuentan con otro conector RJ45 para la conexión adicional de una PC con el objetivo de brindar servicios de Red. En la figura 1.2 se muestra un aparato telefónico IP típico.

Fig. 1.2 Teléfono IP Cisco (Fuente: <http://www.cisco.com/en/US/products/ps7062/index.html>)

- **Adaptadores analógicos IP:** Los adaptadores analógicos IP son dispositivos que permiten la conexión de un teléfono analógico para la conversión de sus señales analógicas a digitales. En la figura 1.3 se muestra un adaptador analógico – digital típico.



LINKSYS PAP2

Fig. 1.3 Adaptador analógico (Fuente: Curso voz sobre IP y asterisk v1.0. Módulo I)

- **Softphones:** Son programas creados con el objetivo de permitir las llamadas desde el ordenador utilizando tecnologías VoIP, existen tanto para sistemas operativos Windows y sistemas Unix. El dibujo de la figura 1.4 muestra unos ejemplos de

Softphones.



Fig. 1.4 Softphones (Fuente: Curso voz sobre IP y asterisk v1.0. Módulo I)

- **Centralitas IP:** Las centralitas IP son dispositivos de telefonía que permiten utilizar de forma combinada la tecnología VoIP (mixtas) o exclusivamente IP (puras). La figura 1.5 muestra unas centralillas IP típicas.

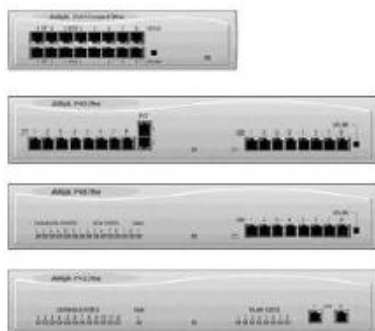


Fig. 1.5 Centralillas IP (Fuente: Curso voz sobre IP y asterisk v1.0. Módulo I)

1.3.1.4 Funcionamiento general de un sistema VoIP con protocolo SIP.

La comunicación SIP se realiza entre lo que se denominan “Agentes de Usuario SIP” o “usuario SIP”, “Servidores de Registro” o “SIP Server” y “SIP Proxy”

- **Usuarios SIP:** Un usuario SIP puede ser una aplicación de mensajería, un *softphone*, un teléfono IP o cualquier dispositivo o software compatible con SIP y que tenga la capacidad de “registrarse” con una cuenta SIP. Los usuarios SIP reciben una URI (*Uniform Resource Identifier*) formada por “usuario”@“dominio” (similar a la de un correo electrónico) donde el campo dominio se corresponde con el Servidor SIP donde se encuentra registrado.
- **Servidor SIP:** Un servidor SIP es una aplicación o dispositivo que permite crear y gestionar cuentas SIP y permitir que los Usuarios SIP se “registren” almacenando la dirección IP donde deben acceder para realizar la comunicación con este usuario.
- **Proxy SIP:** Un Proxy SIP es una aplicación que permite que cualquier usuario SIP envíe un comando a otro usuario SIP.

Los pasos a seguir para el establecimiento de una llamada VoIP con protocolo SIP son:

- **Paso 1:** Los dos comunicantes se registran en el servidor VoIP con sus teléfonos IP o Softphones.
- **Paso 2:** El equipo del emisor pregunta por el equipo del receptor.
- **Paso 3:** El servidor VoIP devuelve datos de contacto al emisor (puertos, direcciones IP).
- **Paso 4:** Se establecen comunicación entre los interlocutores. Todo ello utilizando un protocolo determinado: SIP, IAX2, H323. (Asterisk)

A continuación se explica brevemente cómo funciona el establecimiento de una llamada en VoIP con protocolo SIP. Los términos principales que se usarán serán los siguientes:

- **INVITE:** establece una sesión.
- **ACK:** confirma la solicitud INVITE.
- **BYE:** finaliza una sesión.
- **CANCEL:** cancela el establecimiento de una sesión.
- **REGISTER:** comunica la localización de usuario (nombre de equipo, IP).
- **OPTIONS:** comunica la información acerca de las capacidades de envío y recepción de teléfonos SIP.

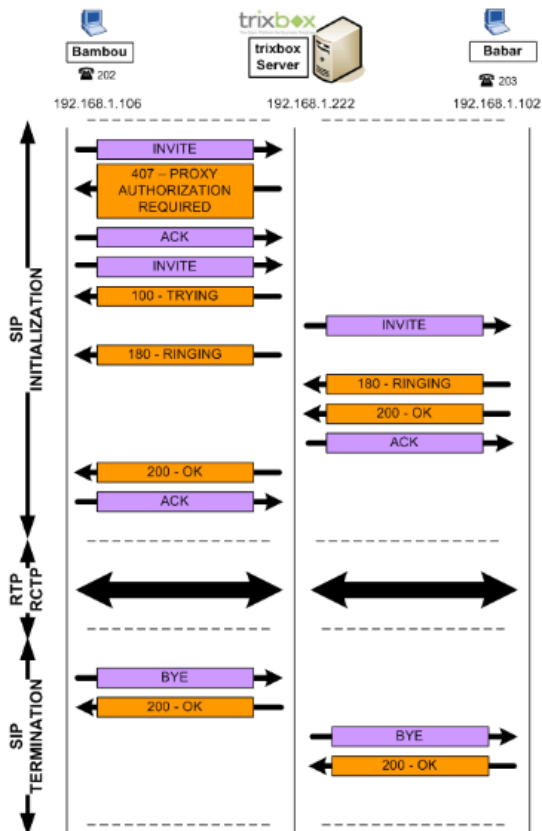


Fig. 1.6. Ejemplo de establecimiento de llamada (Fuente: http://www.openmaniak.com/trixbox_analyze.php#step1)

En la figura 1.6 el teléfono 202 (Bambou) solicita la llamada mediante un INVITE, y a su vez es solicitado a dar su autenticación por el servidor proxy SIP, este mediante un ACK confirma su autenticación y vuelve a enviar un INVITE pero esta vez con toda su información incluida, el teléfono 203 (babar) recibe esta información y establece la llamada y comienza a sonar (180 *ringing*), se confirma la llamada al otro teléfono el momento en el que es levantado el teléfono 203 (200 OK), se vuelve a enviar un ACK desde el teléfono 202 y mediante el protocolo RTP los datos son transmitidos; cuando finaliza la llamada el teléfono 202 envía un BYE y el otro responde con un OK.

1.3.2 Videovigilancia IP.

Hoy en día, la vigilancia IP se ha convertido en la solución tecnológica de seguridad que ofrece control y monitoreo avanzado frente al monitoreo tradicional basado en el sistema de circuito cerrado de televisión CCTV. La vigilancia IP está basada en cámaras que usan el protocolo IP. Tales cámaras pueden formar parte esencial de lo que se denomina Sistema de Video Vigilancia. En el sistema pueden considerarse funciones tales como: grabación de video y audio, detección de eventos en tiempo real; entre otros.

1.3.2.1 Sistemas de Videovigilancia.

Sistemas de circuito cerrado de televisión.

Este sistema se venía utilizando durante varios años y consistía en cámaras analógicas conectadas a un multiplexor mediante cable coaxial, del multiplexor salían señales a un VCR (*Video Camera Recorder*) para el almacenamiento de video en cintas magnéticas. Todo este sistema implicaba una compleja implementación. En la figura 1.7 se tiene un esquema de este sistema

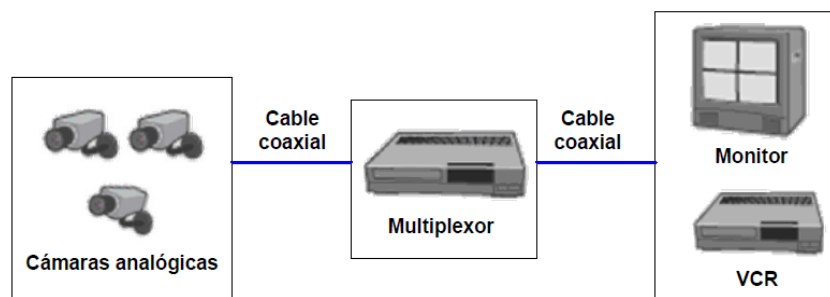


Fig. 1.7 Esquema de Video Vigilancia Analógica (Fuente: <http://biblioteca.epn.edu.ec/catalogo/fulltext/CD-1239.pdf>)

CCTV usando DVR

En estos sistemas se usa un grabador de video digital (DVR) que capta el video, lo digitaliza y lo almacena en un disco duro de manera comprimida, el DVR puede tener características

IP y se puede monitorear remotamente. En la figura 1.8 se muestra un esquema típico de este sistema

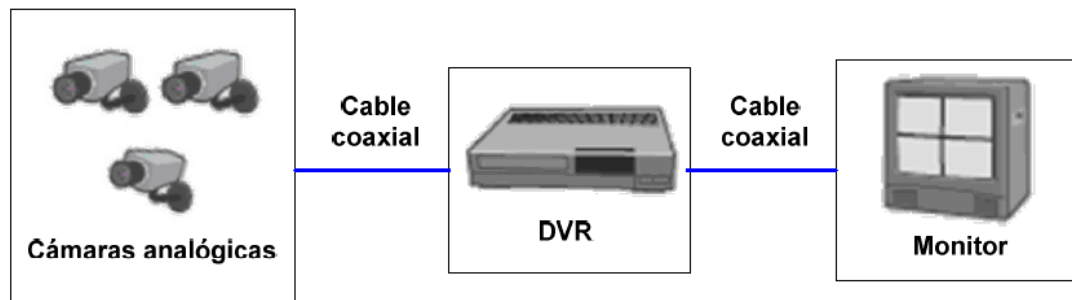


Fig. 1.8 Esquema de Video Vigilancia analógico con DVR (Fuente: <http://biblioteca.epn.edu.ec/catalogo/fulltext/CD-1239.pdf>)

Sistemas de video IP que utilizan servidores de video.

En este tipo de configuración las cámaras que se usan son de tipo analógicas y para usarse en protocolos IP es necesario la implementación un video server para la digitalización de las señales con el fin de poder transmitir por la red. El dibujo de la figura 1.9 muestra un esquema típico de este sistema.

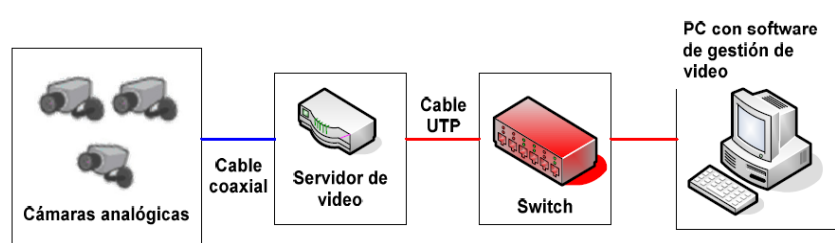


Fig. 1.9 Esquema de Videovigilancia con servidor de video (Fuente: <http://biblioteca.epn.edu.ec/catalogo/fulltext/CD-1239.pdf>)

Sistemas de video-vigilancia IP.

Los sistemas con cámaras IP se conectan directamente a la red y son monitoreadas desde internet o una red LAN conectadas a una PC que funciona como administrador de cada cámara. La figura 1.10 muestra el esquema básico de este sistema, el cual se implementará en este diseño.

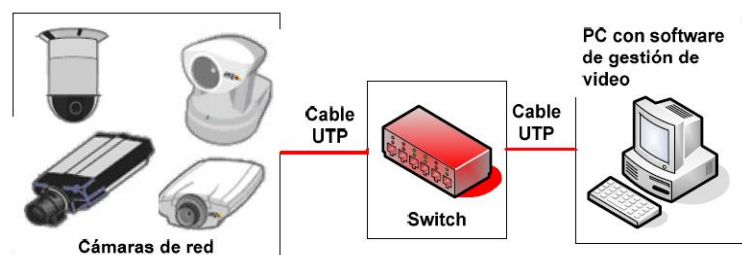


Fig. 1.10 Esquema de video vigilancia IP (Fuente: <http://biblioteca.epn.edu.ec/catalogo/fulltext/CD-1239.pdf>)

Tipos de cámaras IP.

Las cámaras de red IP se pueden clasificar en función de su diseño para uso en interiores o exteriores. En ambos casos las cámaras tendrán sus debidas protecciones para sus diferentes tipos de uso. Ambos tipos de cámaras tanto interiores como exteriores pueden clasificarse en:

Cámaras de red fijas.- Tienen un campo de visión fijo una vez que son montadas. Este tipo de cámaras son usadas en lugares donde se necesite que la cámara sea visible, por ejemplo, en instituciones financieras o lugares en donde se quiera dar a conocer que el local se encuentra bajo vigilancia. (figura 1.11).



Fig. 1.11 Cámaras de red fijas que incluyen versiones inalámbricas y megapíxel (Fuente: http://www.axis.com/es/products/video/camera/about_cameras/types.htm)

Cámaras de red domo fijas.- Son cámaras pre instaladas en carcasas tipo domo, que pueden enfocar el punto seleccionado en cualquier dirección, este tipo de cámaras son muy discretas ya que no se puede apreciar ni ver en qué dirección están apuntando, por ejemplo, son usadas en locales comerciales. (figura 1.12).



Fig. 1.12 Cámaras de red domo fijas. De izquierda a derecha: AXIS 209FD y AXIS 216FD (también disponible en versión reforzada y megapíxel), AXIS P3301 y AXIS 225FD. (Fuente: http://www.axis.com/es/products/video/camera/about_cameras/types.htm)

Cámaras PTZ y cámaras domo PTZ.- Estas pueden moverse horizontalmente, verticalmente y acercarse o alejarse de un área o un objeto de forma manual o automática. Todos los comandos PTZ se envían a través del mismo cable de red que transmite el vídeo, permiten movimientos horizontales de 360° y verticales de 180° y son usadas en lugares discretos donde se necesita esconder hacia donde apuntan las cámaras (figura 1.13).



Fig. 1.13 Cámaras de red domo PTZ. De izquierda a derecha: AXIS 231D+, AXIS 232D+, AXIS 233D. (Fuente: http://www.axis.com/es/products/video/camera/about_cameras/types.htm)

1.3.2.2 Diferencias entre CCTV (analógico) y VideoVigilancia IP.

La Videovigilancia IP ofrece toda funcionalidad frente al sistema clásico de Videovigilancia. A continuación en la tabla 1.2 se destacan las principales diferencias entre los dos sistemas.

	CCTV (analógico)	Vigilancia IP (digital)
Costo	Tendencia a usar cables coaxiales, cuyo uso resulta caro. Gran longitud de cable. Las cámaras pueden ser caras.	Utiliza el cableado Ethernet existente. Requiere menos cable. Las cámaras IP son más asequibles.
Resolución	Las cámaras CCTV ofrecen una mejorada calidad de imagen, pero no soporte para resoluciones de imágenes en mega píxeles.	Soporte para numerosas resoluciones de imagen, incluidas tanto la resolución CCTV analógica estándar como la mega píxel.
Escalabilidad y flexibilidad	Puede resultar complejo de instalar puesto que el cable de las cámaras CCTV puede tener una longitud de cientos de metros. La ampliación requiere agregar capacidad a las cámaras a veces en unidades de 16 y cable adicional	Fácil convergencia a una infraestructura de cableado IP nueva o ya existente. Desarrollo fácil y flexible. PoE permite situar la cámara prácticamente en cualquier sitio. Muy escalable. Puede configurarse para satisfacer las necesidades concretas.
Funcionalidad	Muchas de las cámaras analógicas carecen de las características mas avanzadas, como, por ejemplo, zoom digital.	Permite integrar vigilancia por video con otros sistemas y funciones como: control de acceso, sistemas de alarma, gestión del edificio, gestión del tráfico, etc. Envía avisos automáticos por correo electrónico en tiempo real, de textos o transferencia de archivos como respuesta a la detección de movimiento por la imagen.

Tabla 1.2 Diferencias entre CCTV analógico y Video Vigilancia IP (Fuente: <http://teleinfo-ap.com.mx/site/?p=933>)

1.3.3 Seguridad contra incendios

Los sistemas de alarma contra incendios sirven para alertar a las personas que se encuentran en el interior de un edificio para la evacuación del mismo en caso de incendios, además de notificar a un personal de emergencia o del mismo edificio para tomar las debidas precauciones. Estos sistemas de alarma funcionan con la implementación de sensores de humo, calor o manualmente mediante pulsantes que se encuentran en lugares específicos. Los sensores al ser activados envían una señal al panel central de alarma que informa al personal de emergencia y hace sonar una sirena en el edificio, en algunos casos incluyen luces que indican la emergencia.

En el mercado existen varios tipos de alarma con diferentes características, y actualmente existen comunicadores IP que permiten la transmisión de datos de los paneles de alarma a una red LAN o de internet con la información que generan los sensores en caso de un incendio. Los sistemas de alarma contra incendio se pueden clasificar en:

SISTEMAS CONVENCIONALES.- Se basan en la agrupación de sensores o dispositivos para clasificarlos por zonas, el momento de un incendio la central es informada por la zona en la que se efectuó, pero no puede reconocer en qué lugar exactamente sucedió, por lo que se requiere de una inspección visual. La figura 1.14 muestra la configuración básica de este sistema.



Fig. 1.14 Funcionamiento de un Sistema de Alarmas Convencional (Fuente: www.nws.pe/alarmaincendio2.pdf)

SISTEMAS DIRECCIONABLES.- Este tipo de sistemas envían la señal de alerta al panel de control y mediante un rastreo alfanumérico se puede dar la ubicación del lugar exacto en donde sucedió el evento. El dibujo de la figura 1.15 muestra la configuración básica de un sistema de tipo direccionable.

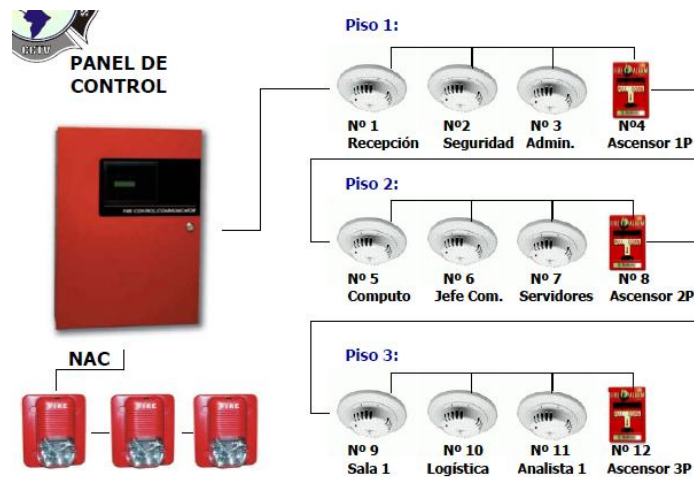


Fig. 1.15. Funcionamiento de un Sistema de Alarmas Direccional (Fuente: www.nws.pe/alarmaincendio2.pdf)

La mayoría de los paneles de alarma tienen la posibilidad de conectarse a una central de monitoreo remoto, empleando una línea telefónica, que al conectarse transmite la información de alerta a la central mediante tonos DTMF, este tipo de comunicación utiliza el protocolo *Contact ID*; actualmente estos tipos de alarmas pueden comunicarse a una red IP para la transferencia de información. Este contacto lo realiza el panel de control mediante un comunicador IP basado en una tarjeta de interfaz para la transmisión de los datos.

1.3.3.1 Elementos que intervienen en un Sistema de Alarma Contra Incendios.

Comunicador IP.- Este dispositivo es una tarjeta de interfaz que permite el monitoreo de paneles de alarma a través de Internet o en una red LAN, dispositivos de hardware con capacidad para telecontrol. El comunicador IP brinda además información para el monitoreo de la conexión IP. (Figura 1.16)

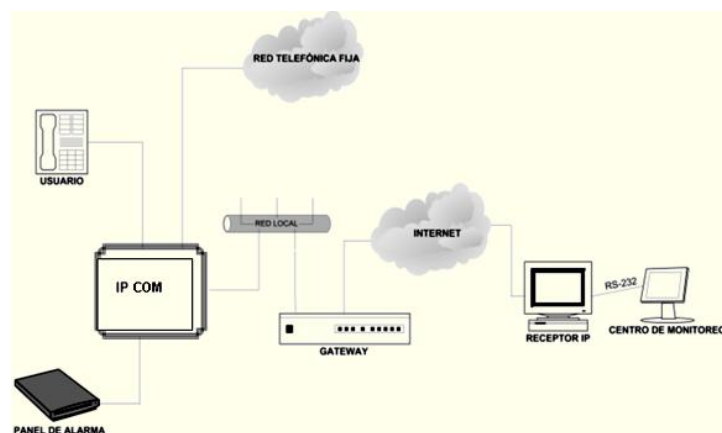


Fig. 1.16 Configuración de equipos para alarma contra incendios (Fuente: http://www.avatec.com.ar/comunicador_ip01.htm)

Este tipo de comunicador IP funciona en dos modos: modo de interceptación y modo de backup telefónico. Cuando se encuentra en modo de interceptación este intercepta todas las alertas de alarma y las transmite mediante una red LAN o internet. Cuando el panel de alarma detecta un evento y quiere comunicarlo, el comunicador IP toma el lugar de la central de monitoreo y envía los tonos de inicio de protocolo cuando el panel recibe tono de invitación a discar, esto sucede en alarmas que se comunican con una línea telefónica.

El Comunicador IP soporta (*Contact-ID* y *Radionics (4x2)*), protocolos que usa para transmitir los eventos. Después de recibir y entender el protocolo, el comunicador IP envía ese evento a través de un paquete IP para el centro de monitoreo IP y se queda aguardando la recepción de un paquete de respuesta del centro de monitoreo. Al recibir el paquete de respuesta, el comunicador IP envía al panel la señal de recepción correcta del evento, de esa forma se garantiza que el panel sólo va a considerar el evento transmitido en caso que el paquete haya sido bien recibido por el centro de monitoreo.

El comunicador IP garantiza que el vínculo IP se mantenga con el envío cada 60 segundos de un paquete llamado HEART BEAT, cada vez que el sistema de monitoreo reciba un paquete del comunicador IP, envía como respuesta un paquete (RE); en caso de que el comunicador IP no reciba tres respuestas a tres paquetes HEART BEAT consecutivos se considera que el vínculo se perdió y pasa a funcionar en modo de BACKUP TELEFÓNICO que utiliza la red de telefonía en vez de Internet para el envío de eventos.

Panel de alarma

El panel de alarma está diseñado para cubrir las necesidades más exigentes del mercado residencial, cuenta con zonas inalámbricas, códigos de usuario memoria de eventos, salida de sirena, comunicador telefónico para centrales telefónicas de alarma, compatible con interfaces de monitoreo de tercera generación, TCP/IP y celular GPRS. La figura 1.17 muestra un panel típico de alarma contra incendios.



Figura 1.17 Panel de Alarma honeywell Silent night (Fuente: <http://www.silentknight.com/products/5600.html>)

Detector de Humo Fotoeléctrico



Fig. 1.18 Detector de Humo Fotoeléctrico (Fuente: <http://www.silentknight.com/products>)

Detectan Humo a través del principio de difusión de la luz., se basan en una fuente emisora de luz y un elemento fotosensible, acomodados dentro de una cámara de detección para que un rayo de luz no impacte un elemento directamente. Cuando las partículas de Humo entran en la cámara, harán que la luz sea reflejada y no llegue al elemento, activando la alarma. El dibujo de la figura 1.19 muestra el principio de funcionamiento de los sensores de humo.

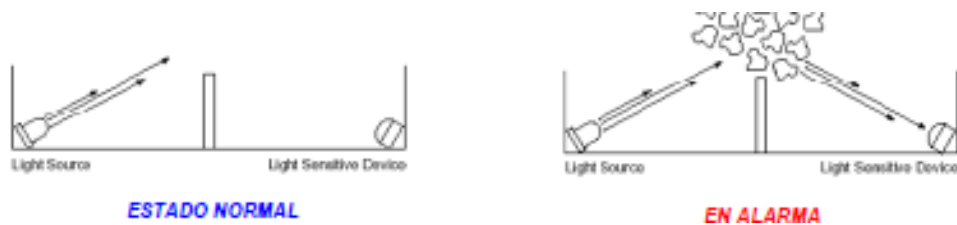


Fig. 1.19 Principio de funcionamiento Sensores de humo (Fuente: www.nws.pe/alarmaincendio2.pdf)

CAPÍTULO II

REQUERIMIENTOS DE LA RED

El presente capítulo describe los requerimientos del edificio realizando un análisis de las aplicaciones y puertos de red en cada planta para obtener los datos necesarios y realizar el cálculo del ancho de banda de internet estimado que se brindara en el edificio así como el estimado de cámaras, AP y demás elementos que conformaran la red del edificio.

2.1 Requerimiento de aplicaciones y puntos de red de la planta baja

En la tabla 2.1 se aprecia las necesidades de cada departamento de la planta baja, tales como Telefonía IP, telefonía IP con servicio de internet (teléfonos que se pueden conectar a una PC debido a que tienen 2 puertos de red), internet, red, access point, y sensores de humo; considerando en ciertas ubicaciones puntos de red extras que estarán disponibles para cualquier aplicación, como en la sala de entrenadores, sala de control, bodega, etc.

Tabla 2.1 Número de aplicaciones y puntos de red de la planta baja.

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP	SH
1	Cocina	1					1
2	Repostería	1					
3	Despensa	1					1
4	Comedor					1	
5	Almacén 1		1				1
6	Almacén 2		1				1
7	Almacén 3		1				1
8	Almacén 4		1				1
9	Almacén 5		1				1
10	Almacén 6		1				1
11	Sala de Prensa		1				
12	Sala de Internet			5			
13	Sala de reuniones				1		
14	Recepción		1		1		
15	Gerencia		1		1		
16	Contabilidad	2			2		1
17	Secretaría	1	1		2		1
18	Sala VIP	1					
19	Cafetería	1				1	
20	Cocina						1
21	Habitaciones 1-5	5					1
22	Habitaciones 6-9	4				1	1
23	Habitaciones 10-13	4					1
24	Piscina					2	
25	Sala Entrenadores				2		
26	Sala Control				1		
27	Bodega				1		
28	Secado				1		
29	Planchado				1		
30	Recepción	1					
31	Vestíbulo Derecho					1	
	TOTAL	22	10	5	13	6	14

En la tabla 2.1.1 se muestra la ubicación de las cámaras IP que se implementarán en esta planta.

Tabla 2.1.1 Cámaras IP a utilizarse en la planta baja

Sector	Número de Cámaras
Comedor	2
Vestíbulo Entrada Izquierdo	1
Pasillo 1	1
Vestíbulo Entrada Principal	1
Recepción	1
Contabilidad	1
Vestíbulo Entrada Derecho	1
Pasillo Habitaciones	2
Piscina-Pasillo-Gimnasio	4
TOTAL	14

En la figura 2.1 se muestra la topología de red que se utilizará para la planta baja. Como se puede apreciar se utiliza un esquema en cascada.

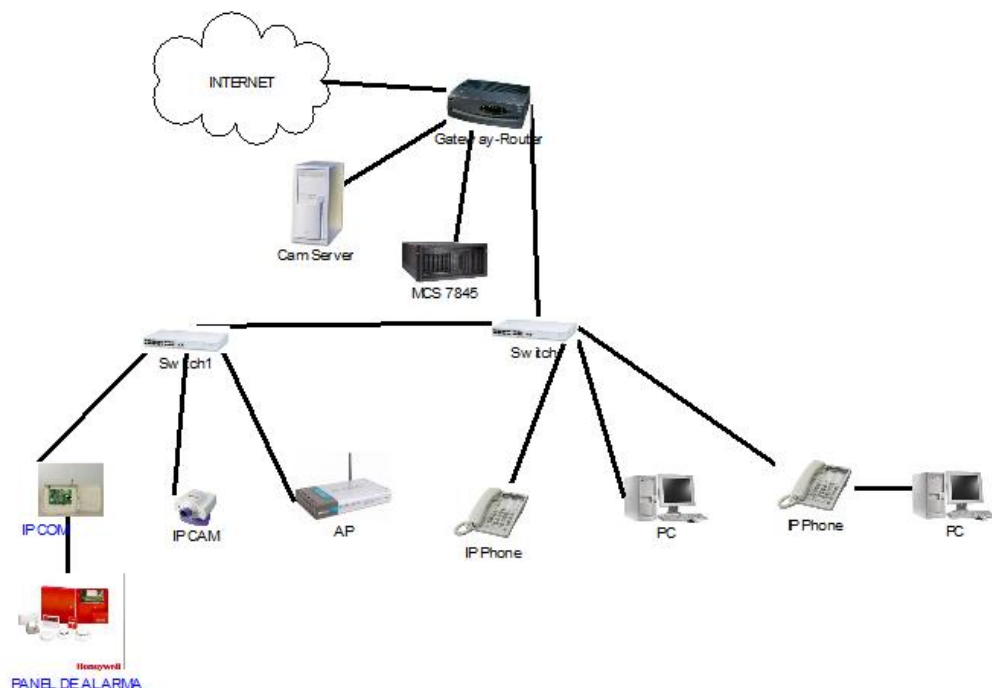


Fig. 2.1 Topología de red general de la planta baja.

2.2 Requerimiento de aplicaciones y puntos de red de la primera planta.

La tabla 2.2 muestra los puntos de red que se utilizarán en la primera planta alta, a partir de esta planta se encuentran solo habitaciones por lo que se colocan Access Points (APs) en cada pasillo del piso para brindar servicio de internet a los usuarios, así como cámaras ubicadas en puntos estratégicos para garantizar la vigilancia.

Tabla 2.2 Número de aplicaciones y puntos de red de la primera planta.

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP	SH
1	Habitaciones 14-17	4					1
2	Habitaciones 18-21	4				1	1
3	Habitaciones 22-25	4					2
4	Habitaciones 26-30	5				1	1
5	Habitaciones 31-34	4					1
6	Habitaciones 35-40	6				1	2
7	Habitaciones 41-44	4					1
8	Habitaciones 45-49	5				1	2
9	Habitaciones 50-53	4				1	1
10	Habitaciones 54-57	4					1
11	Habitaciones 58-61	4					1
	TOTAL	48				5	14

En la tabla 2.2.1 se muestra la ubicación de las cámaras IP que se implementarán en esta planta.

Tabla 2.2.1 Cámaras IP a utilizarse en la primera planta

Sector	Número de Cámaras
Pasillo Habitaciones Lateral Izquierdo	1
Vestíbulo Izquierdo	1
Pasillo Habitaciones Izquierdo	1
Vestíbulo Central	1
Pasillo Habitaciones Derecho	1
Vestíbulo Entrada Derecho	1
Pasillo Habitaciones Lateral Derecho	1
TOTAL	7

En la figura 2.2 se muestra la topología de red que se utilizará para la primera planta alta. Como se puede apreciar se utiliza también un esquema en cascada.

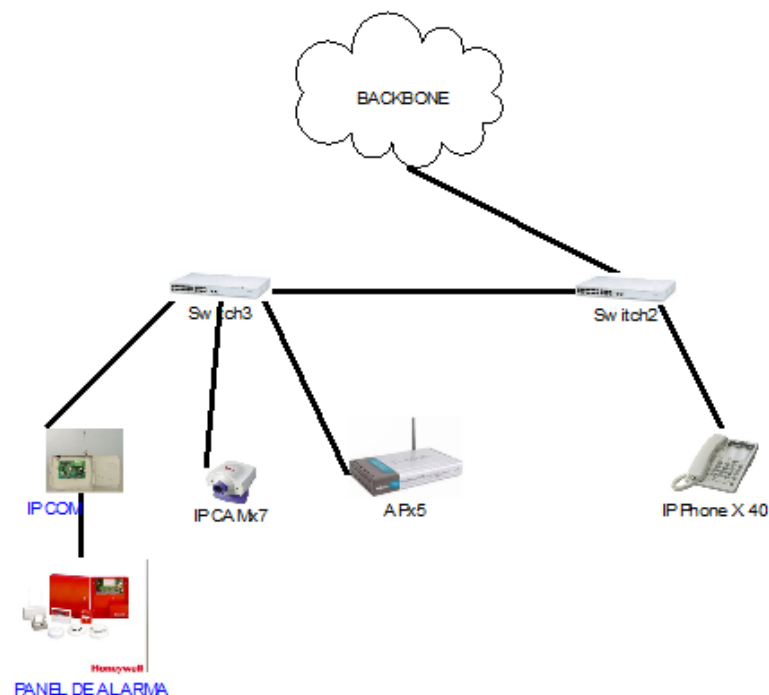


Fig. 2.2. Topología de red general de la primera planta.

2.3 Requerimiento de aplicaciones y puntos de red de la segunda planta.

A partir de la segunda planta alta el edificio se divide en 2 partes que denominaremos: segunda planta (A) y segunda planta (B) tratándolos como pisos independientes ya que cada uno tendrá su rack de comunicaciones. La tabla 2.3 muestra los requerimientos de la segunda planta (A)

Tabla 2.3 Número de aplicaciones y puntos de red de la segunda planta (A)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP	SH
1	Habitaciones 62-64	3					1
2	Habitaciones 65-68	4				1	1
3	Habitaciones 69-72	4					1
4	Habitaciones 73-77	5				1	2
5	Habitaciones VIP 1-2	2		2			2
6	Habitaciones 78-81	4					1
7	Habitaciones 82-85	4				1	1
8	Habitaciones 86-89	4					1
	TOTAL	30		2		3	10

La tabla 2.3.1 muestra la distribución de cámaras a usarse en esta planta.

Tabla 2.3.1 Cámaras IP a utilizarse en la segunda planta (A)

Sector	Número de Cámaras
Pasillo Habitaciones Lateral Izquierdo	1
Vestíbulo Izquierdo	1
Pasillo Habitaciones Izquierdo	1
TOTAL	3

En la figura 2.3 se muestra la topología de red que se utilizará para la segunda planta (A) Como se puede apreciar se utiliza también un esquema en cascada.

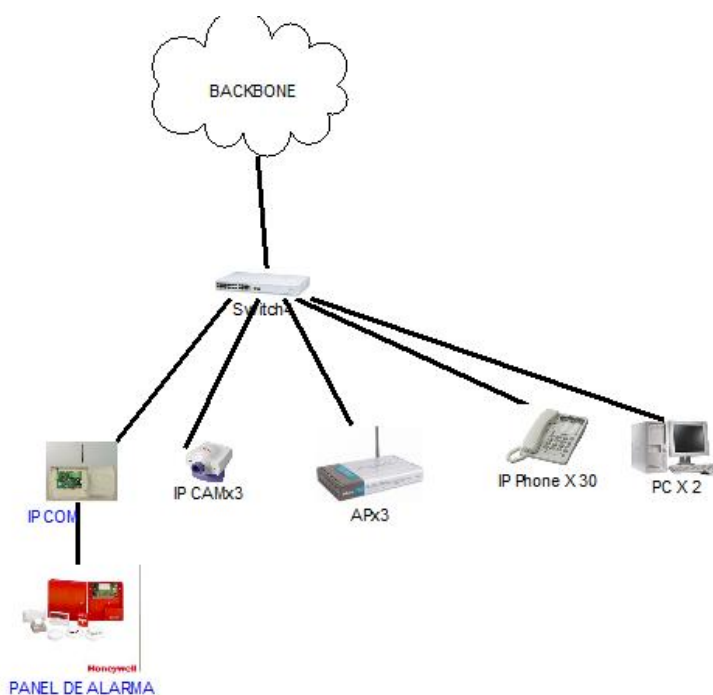


Fig. 2.3 Topología de red general de la segunda planta (A)

La tabla 2.3.2 muestra el los requerimientos de red de la segunda planta (B)

Tabla 2.3.2 Número de aplicaciones y puntos de red de la segunda planta (B)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP	SH
1	Habitaciones 90-93	4					1
2	Habitaciones 94-97	4				1	1
3	Habitaciones 98-100	3					1
4	Habitaciones VIP 3-4	2		2			2
5	Habitaciones 101-104	4					2
6	Habitaciones 105-108	4				1	1
7	Habitaciones 109-111	3					1
	TOTAL	24		2		2	9

La tabla 2.3.3 muestra las cámaras IP se utilizarán en esta planta.

Tabla 2.3.3 Cámaras IP a utilizarse en la segunda planta (B)

Sector	Número de Cámaras
Pasillo Habitaciones Lateral Derecho	1
Vestíbulo Derecho	1
Pasillo Habitaciones Derecho	1
TOTAL	3

La figura 2.4 muestra la topología de red de esta planta, una topología tipo cascada.

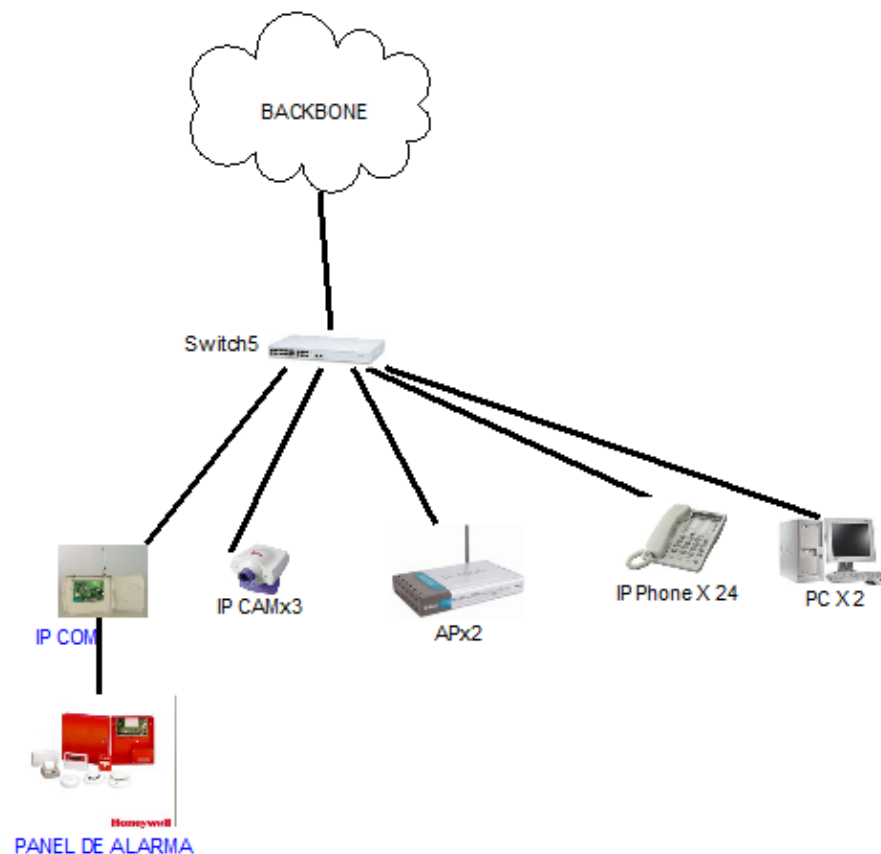


Fig. 2.4. Topología de red general de la segunda planta (B)

2.4 Requerimiento de aplicaciones y puntos de red de la tercera planta alta

La tabla 2.4 muestra los puntos de red que se utilizarán en la tercera planta (A).

Tabla 2.4 Número de aplicaciones y puntos de red de la tercera planta (A)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP	SH
1	Habitaciones 112-114	3					1
2	Habitaciones 115-118	4				1	2
3	Habitaciones 119-122	4					1
4	Habitaciones 123-125	3				1	1
5	Habitaciones VIP 5-6	2		2			2
6	Habitaciones 126-129	4					1
7	Habitaciones 130-135	6				1	1
	TOTAL	26		2		3	9

La tabla 2.4.1 muestra la distribución de cámaras a usarse en esta planta.

Tabla 2.4.1 Cámaras IP a utilizarse en la tercera planta (A)

Sector	Número de Cámaras
Pasillo Habitaciones Lateral Izquierdo	1
Vestíbulo Izquierdo	1
Pasillo Habitaciones Izquierdo	1
TOTAL	3

La figura 2.5 muestra la topología de red en esta planta, una topología en cascada

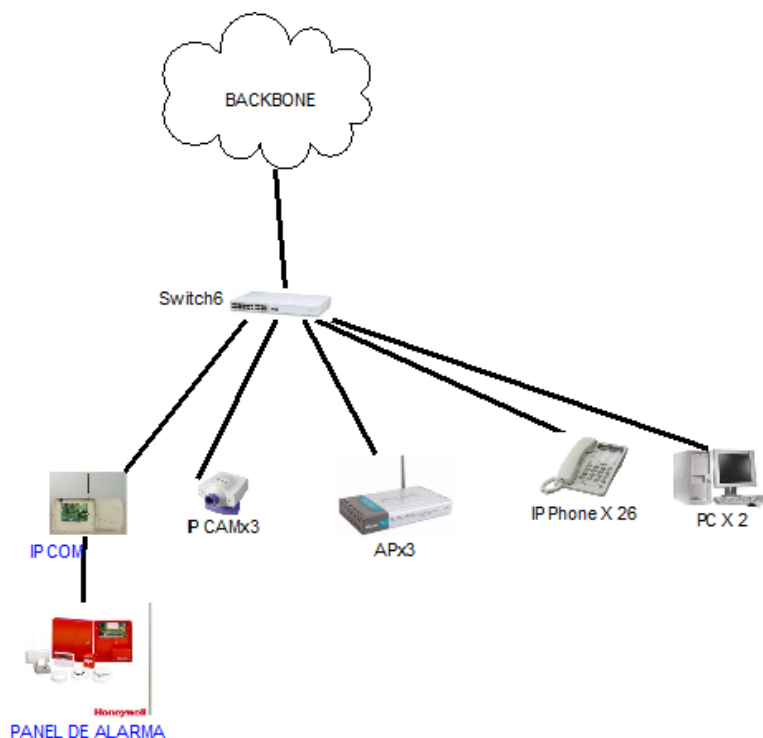


Fig. 2.5 Topología de red general de la tercera planta (A)

La tabla 2.4.2 muestra los requerimientos de la tercera planta (B)

Tabla 2.4.2 Número de aplicaciones y puntos de red de la tercera planta (B)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP	SH
1	Habitaciones 136-139	4					1
2	Habitaciones 140-144	5				1	2
3	Habitaciones VIP 7-8	2		2			2
4	Habitaciones 145-148	4					1
5	Habitaciones 149-153	5				1	2
	TOTAL	20		2		2	8

La tabla 2.4.3 muestra la distribución de cámaras en esta planta

Tabla 2.4.3 Cámaras IP a utilizarse en la tercera planta (B)

Sector	Número de Cámaras
Pasillo Habitaciones Lateral Derecho	1
Vestíbulo Derecho	1
Pasillo Habitaciones Derecho	1
TOTAL	3

La figura 2.6 muestra la topología de red a implementarse en esta planta, una topología tipo cascada.

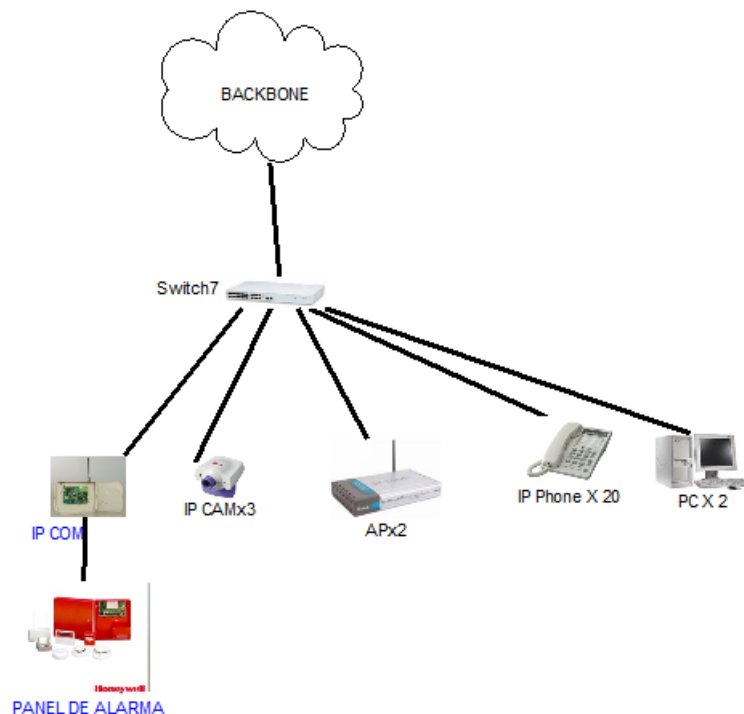


Fig. 2.6 Topología de red general de la tercera planta (B)

2.5 Requerimiento de aplicaciones y puntos de red de la cuarta y quinta planta.

Conforme se conoció el edificio, una parte de la cuarta planta fue reservada para la colocación de oficinas extras (oficinas que no constan en los planos originales), así que en este caso se procedió en colocar por oficina 1 teléfono IP y puntos de red que podrán ser utilizados para cualquier aplicación que se desee, la quinta planta se unifica con los equipos

de comunicaciones de la cuarta planta debido a que solo hay 4 habitaciones VIP que pueden bajar directamente al TC (Cuarto de Telecomunicaciones) de la cuarta planta.

En tabla 2.5 se puede apreciar los puntos de red que se usarán en la cuarta planta (A) y quinta planta (A)

Tabla 2.5 Número de aplicaciones y puntos de red de la cuarta planta (A) y quinta planta (A)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP	SH
1	Oficina extra 1	1			1		1
2	Oficina extra 2	3			3		
3	Oficina extra 3	1			1		1
4	Oficina extra 4	1			2		
5	Oficina extra 5	1			2		1
6	Oficina extra 6	1			2		
7	Oficina extra 7	1			2		
8	Bar extra						1
9	Habitaciones VIP 9-10	2		2			2
10	Habitaciones 154-157	4				1	1
11	Habitaciones 158-161	4					2
QUINTA PLANTA (A)							
1	Habitaciones VIP 13-14	2		2			2
	TOTAL	21		4	13	1	11

La tabla 2.5.2 muestra la distribución de cámaras IP a usarse en estas plantas.

Tabla 2.5.1 Cámaras IP a utilizarse en la cuarta planta (A) Y quinta planta (A)

Sector	Número de Cámaras
Vestíbulo Izquierdo	1
Pasillo Habitaciones Izquierdo	1
Vestíbulo Izquierdo Quinta Planta	1
TOTAL	3

La figura 2.7 muestra la topología de red tipo cascada a implementarse en estas plantas.

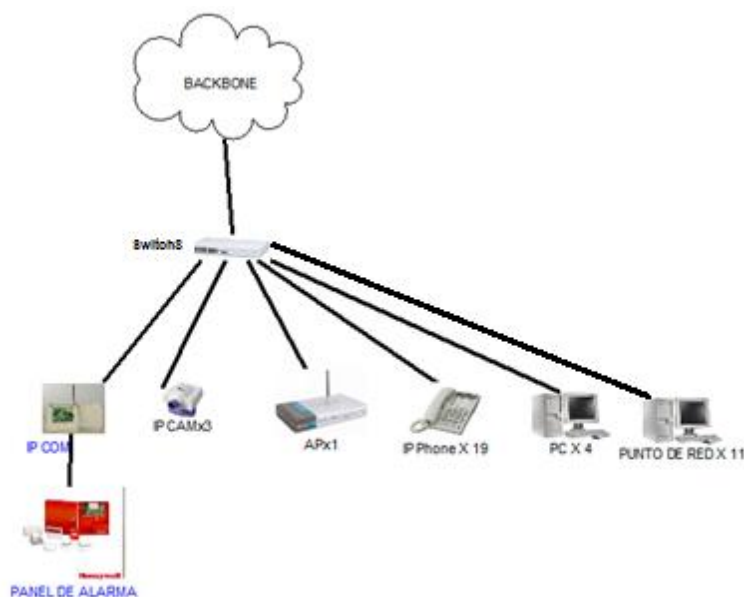


Fig. 2.7 Topología de red general de la cuarta y quinta planta (A)

La tabla 2.5.2 muestra los requerimientos de la cuarta y quinta planta (B)

Tabla 2.5.2 Número de aplicaciones y puntos de red de la cuarta planta (B) Y quinta planta (B)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP	SH
1	Habitaciones 162-165	4					1
2	Habitaciones 166-168	3				1	2
3	Habitaciones VIP 11-12	2		2			2
4	Habitaciones 169-172	4					1
5	Habitaciones 173-177	4				1	2
QUINTA PLANTA (B)							
1	Habitaciones VIP 15-16	2		2			2
	TOTAL	19		4		2	10

La tabla 2.5.3 muestra la distribución de cámaras a usarse en estas plantas.

Tabla 2.5.3 Cámaras IP a utilizarse en la cuarta planta (B) Y quinta planta (B)

Sector	Número de Cámaras
Vestíbulo Derecho	1
Pasillo Habitaciones Derecho	1
Pasillo Habitaciones Lateral Derecho	1
Vestíbulo Derecho Quinta Planta	1
TOTAL	4

La figura 2.8 muestra la topología de red tipo cascada a implementarse en estas plantas.

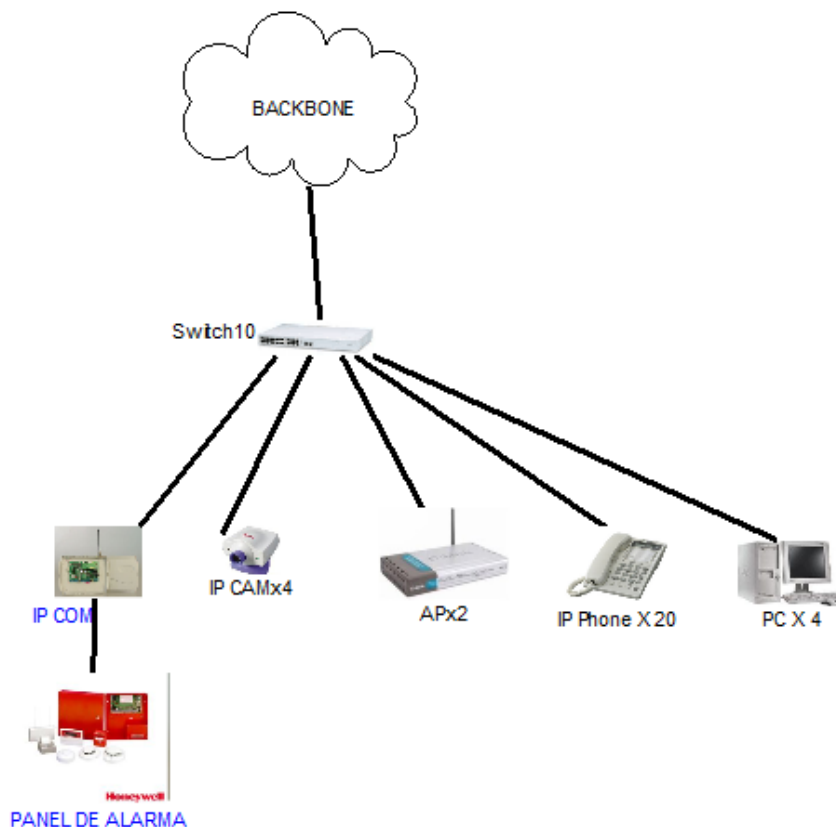


Fig. 2.8 Topología de red general de la cuarta y quinta planta (B)

2.6 Requerimientos totales de aplicaciones y puertos de red para el Centro de Alto Rendimiento (CAR) de Totoracocha.

Luego de realizar el respectivo análisis por cada planta se concluye con los resultados de la tabla 2.6 para el total de puertos y aplicaciones del edificio. En los anexos 8-14 se encuentran los planos de cada planta del edificio con su respectivo cableado de red y diagrama vertical.

Tabla 2.6 Total de puertos y aplicaciones del edificio.

DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNE T 128kbps	RED	AP	S H	CÁMARA S IP
Planta Baja	22	10	5	13	6	14	14
Primera Planta	48				5	14	7
Segunda Planta (A)	30		2		3	10	3
Segunda Planta (B)	24		2		2	9	3
Tercera Planta (A)	26		2		3	9	3
Tercera Planta (B)	20		2		2	8	3
Cuarta Planta (A) y Quinta Planta (A)	21		4	13	1	11	3
Cuarta Planta (B) y Quinta Planta (B)	19		4		2	10	4
TOTAL	210	10	21	26	24	85	40

2.7 Cálculo de tráfico de ancho de banda de internet.

Para este estudio se considera un ancho de banda estimado para el edificio, tomando en cuenta a los usuarios que se conectan directamente con cable de red y usuarios que harán uso de los Access Point. Se toma como un estimado de 35 usuarios que tendrán internet por cable de red y 8 el número de usuarios que tendrán acceso a cada AP del edificio, a continuación se detalla el número de usuarios por planta.

Tabla 2.7 Distribución estimada de usuarios por planta.

PLANTA	USUARIOS POR AP	USUARIOS POR CABLE DE RED
Planta Baja	48	15
Primera Planta Alta	40	
Segunda Planta Alta	40	4
Tercera Planta Alta	40	4
Cuarta Planta Alta	24	4
Quinta Planta Alta		4
TOTAL	192	31

El estimado de usuarios se realiza considerando al edificio casi lleno en su capacidad de albergamiento, por lo que el ancho de banda de internet a calcular sería aceptable.

Suponiendo que cada usuario debe tener 128kbps de banda ancha, para cubrir las necesidades de cada usuario se tendría que contratar alrededor de 28Mbps desde el ISP lo cual resulta demasiado costoso. El cálculo de ancho de banda depende de estos factores:

Overbooking.- Es un factor que especifica en cuantos clientes se dividirá el ancho de banda dedicado/efectivo. Se lo utiliza gracias a que cuando un usuario “navega” no está constantemente utilizando el canal, ya que una vez cargado el sitio el enlace queda sin uso, éste tiempo sin uso puede ser utilizado por otro usuario para poder racionalizar el ancho de banda, que por lo general es limitado.

Se le puede dar una escala del 1 al 15 con estos rangos:

- 1.- Excelente: Acceso dedicado
- 5.- Muy bueno: Semi Dedicado
- 8.- Aceptable
- 10.- Normal - Standard
- 15.- Sobre saturado.

Throughput.- Es la capacidad de transferencia real que fluye por un sistema, se toma un 10% como aceptable (estándar) y un 15% para usuarios Premium. El ancho de banda depende de la siguiente fórmula:

$$ABw = \{throughput / overbooking\} \times USUARIOS$$

Tomando en cuenta estos factores de cálculo de ancho de banda se estima los valores a usarse en cada caso.

A los 15 usuarios de cableado directo se brindara 1,5Mbps con un throughput de 15% para considerarlos usuarios Premium ya que tendrán en este caso la menor compresión (5), se considera entre 3 AP (24 usuarios) de la Planta Baja (Pasillo de habitaciones, vestíbulo y cafetería) con un ancho de banda promedio de 512 Kbps con un throughput de 10% y una compresión de 8, los otros 3 AP (24 usuarios) (Piscina-comedor) se dará un ancho de banda promedio de 640kbps, 10% de throughput, compresión de 8.

$$ABw = 102.40 \text{ kbps} / 5 \times 15 + 51.2 \text{ kbps} / 8 \times 24 + 64 \text{ kbps} / 8 \times 24 =$$

$$ABw = 307.200 + 153.60 + 192 = 652.80 \text{ kbps}$$

En la primera planta 3 AP (24 usuarios) con un ancho de banda total de 768kbps throughput de 10% y una compresión de 8, a los otros 2 AP (16 usuarios) 512kbps throughput de 10% y compresión de 7

$$ABw = 76.8 \text{ kbps} / 8 \times 24 + 51.2 \text{ kbps} / 7 \times 16 =$$

$$ABw = 230.4 + 117.02 = 347.42 \text{ kbps}$$

En la segunda planta 3 AP (24 usuarios) con un ancho de banda total de 1Mbps throughput de 10% y una compresión de 8, a los otros 2 AP (16 usuarios) se considera 768kbps throughput de 10% y compresión de 7

$$ABw = 102.4 \text{ kbps} / 8 \times 24 + 76.8 \text{ kbps} / 7 \times 16 =$$

$$ABw = 307 \text{ kbps} + 175.54 = 482.74 \text{ kbps}$$

En la tercera planta se toma 3 AP (24 usuarios) con un ancho de banda total de 1Mbps throughput de 10% y una compresión de 8, a los otros 2 AP (16 usuarios) con 768kbps throughput de 10% y compresión de 7

$$ABw = 102.4\text{kbps}/8 \times 24 + 76.8\text{kbps}/7 \times 16 =$$

$$ABw = 307\text{kbps} + 175.54 = 482.74\text{kbps}$$

En la cuarta planta se considera 3 AP (24 usuarios) (Parte Derecha) con un ancho de banda total de 1,5Mbps throughput de 10% y una compresión de 8

$$ABw = 153.6\text{kbps}/8 \times 24$$

$$ABw = 460\text{ kbps}$$

A partir de la segunda planta alta hasta la quinta planta alta se tienen en total 16 habitaciones VIP las cuales se las toma como usuarios premium y tendrán compresión de 2 (acceso semidedicado) y se brindara 1Mbps

$$ABw = 102.4\text{kbps}/2 \times 16 =$$

$$ABw = 819.2\text{kbps}$$

Total de ancho de banda mínimo

$$ABw_{\text{Total}} = 652.80\text{kbps} + 347.42\text{kbps} + 482.74\text{kbps} + 482.74\text{kbps} + 460\text{kbps} + 860\text{kbps}$$

$$ABw_{\text{total}} = 2754\text{kbps}$$

El mínimo ancho de banda para tratar de cubrir las necesidades de los usuarios de internet no puede ser menor a 2754kbps por lo cual contratar desde el proveedor de internet (ISP) unos 4 o 5 megas es suficiente para brindar un servicio aceptable para navegación de internet.

2.8 Cuartos de Comunicaciones

Los cuartos de telecomunicaciones (TC) son espacios cerrados dentro de un piso de algún edificio. Los equipos y distribuidores del cableado estructurado se deben instalar en áreas con acceso restringido de un edificio, denominados cuarto de equipos o cuarto de telecomunicaciones. Cada edificio debe tener al menos uno de estos cuartos.

Los cuartos de equipos son considerados diferentes a los cuartos de telecomunicaciones, debido a que albergan equipos de mayor importancia, tamaño, capacidad y complejidad. Un cuarto de telecomunicaciones debe tener todos los requerimientos tales como espacio, alimentación eléctrica, entre otras, para la correcta operación de los equipos, además de acceso directo a la canalización principal del edificio y a la canalización horizontal de las oficinas.

La escalabilidad que permite el crecimiento futuro es otro aspecto a tener en cuenta en la configuración del equipamiento. La configuración inicial debe incluir espacio adicional en el bastidor para así poder agregar otros paneles de conexión que permitirá, en el futuro, realizar fácilmente modificaciones a la instalación del cableado. La figura 2.9 muestra la disposición de los cuartos de comunicaciones del diseño.

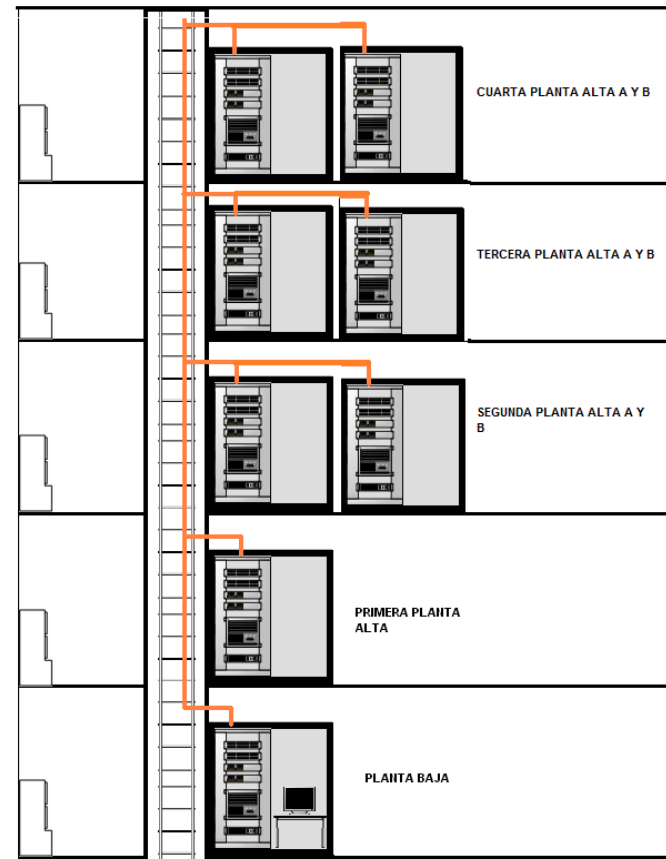


Fig. 2.9 Disposición de los cuartos de comunicaciones

2.9 Equipos a utilizarse en el diseño de red.

A continuación se detallan las características de los equipos a implementarse en el diseño según los requerimientos de la red y la capacidad de los mismos.

2.9.1 Router Cisco 2800 series



Fig. 2.10. Cisco Router 2800 (Fuente:

http://www.cisco.com/en/US/prod/collateral/routers/ps5854/ps5882/product_data_sheet0900aecd8016fa68_ps5854_Products_Data_Sheet.html)

La figura 2.10 muestra un router Cisco 2800 cuyas características más importantes son:

- **Video:** Podrá activar sistemas de vigilancia y seguridad más rentables o admitir medios de *streaming* en vivo o a pedido.
- **Seguridad:** Reduce los riesgos para su empresa relacionados con virus y otras amenazas a la seguridad.
- **Redes privadas virtuales:** Proporciona al personal remoto y a los trabajadores móviles un acceso seguro a los activos de la compañía a través de una conexión segura.
- **Arquitectura modular:** Con una amplia variedad de opciones de LAN y WAN disponibles, podrá actualizar sus interfaces de red para admitir futuras tecnologías. La serie 2800 ofrece varios tipos de ranuras que facilitan la agregación de conectividad y servicios en un futuro conforme su negocio vaya creciendo.
- **Flexibilidad:** La conectividad a través de DSL, módem de cable, tecnología inalámbrica T1 o 3G maximiza las opciones de conexión tanto primarias como de copia de seguridad.
- Tiene Integración con el software *Cisco Unified Communications Manager* para soporte de procesamiento de llamadas de hasta 96 usuarios.
- Mayor confiabilidad y flexibilidad que le permite dar prioridad al tráfico de voz o al intercambio de datos para que la entrega de información se adapte a las necesidades de su empresa.
- Diferentes opciones de conectividad de banda ancha y red.
- Opciones de suministro de energía a los dispositivos de red a través de su conexión Ethernet (*Power Over Ethernet*) para reducir los costos de cableado.
- Cuenta con interfaces FXO para telefonía que sirven para conectar líneas telefónicas de la PSTN directamente al router de manera que funciona como *gateway* para los servicios de telefonía.

Para información más detallada acerca de este equipo visite <http://www.cisco.com/en/US/products/ps5854/index.html>

2.9.2 Switches de la serie Catalyst 2960 de Cisco



Fig. 2.11 Switch Cisco 2960S-24PS-L

(http://www.cisco.com/web/LA/soluciones/comercial/products/routers_switches/catalyst_2960_series_switches/index.html)

Los switches de Cisco Catalyst 2960 (figura 2.11) soportan voz, datos, vídeo y acceso seguro.

Características destacadas:

- **Comunicaciones todas en uno:** Soporte de datos, voz y tecnología inalámbrica, para disponer de una red que admita todas las necesidades de un negocio o empresa.
- **Inteligencia:** Permite la prioridad al tráfico de voz o al intercambio de datos para alinear la entrega de información a sus requisitos de negocio.
- Capacidad de *Power over Ethernet* para poder implementar nuevas funcionalidades como voz y tecnología inalámbrica sin tener que realizar un nuevo cableado.
- Opción de *Fast Ethernet* (transferencia de datos de 100 Mbps) o *Gigabit Ethernet* (transferencia de datos de 1000 Mbps), dependiendo del precio y las necesidades de rendimiento.
- Múltiples modelos de configuración, con la habilidad para conectar escritorios, servidores, teléfonos IP, puntos de acceso inalámbrico, cámaras de TV de circuito cerrado u otros dispositivos de red.
- Funciones de monitorización de red y solución de problemas de conectividad mejoradas.

En este caso de diseño se escoge los switches **2960S-24PS-L** y el switch **2960S-48FPS-L** debido a la característica principal de que sus puertos son PoE (*Power of Ethernet*) lo que simplificaría bastante el tipo de cableado ya que cualquier dispositivo de la red, ya sea un teléfono IP, una cámara IP que tengan la característica de PoE, serán alimentadas eléctricamente por el mismo cable de datos, evitando colocar cada dispositivo de red cerca de una toma eléctrica. Otra característica importante de estos switches es que incluyen 4 puertos SFP de *gigabit Ethernet* que serán de utilidad para realizar el cableado vertical de *backbone* entre planta y planta.

Para características adicionales de este equipo visite <http://www.cisco.com/en/US/products/ps6406/index.html>

2.9.3 Cámara IP para Internet empresarial Cisco PVC2300



Fig. 2.12 Cámara IP PVC2300 (Fuente: <http://www.cisco.com/en/US/products/ps9945/index.html>)

Características Principales:

La cámara IP PVC2300 (figura 2.12) es una cámara de caja con PoE, lentes intercambiables y puertos de E/S que permiten una instalación flexible para varias aplicaciones, contiene códecs duales simultáneos que ofrecen una combinación óptima para la visualización y el almacenamiento de video. Una característica útil para este diseño es que consta de audio bidireccional, multidifusión IP, 3GPP y muchas otras funciones avanzadas que la convierten en una solución ideal para instalaciones de vigilancia.

Al ser un dispositivo con POE puede recibir energía eléctrica de un switch o inyector de corriente PoE a través de los cables Ethernet, esto permite su instalación cerca de cielorrasos, encima de techos o en cualquier lugar donde no haya tomacorrientes disponibles. Además, la cámara incorpora un filtro de corte infrarrojo (IR) que, al utilizarse con una lámpara infrarroja (IR) individual, permite la captura de video en oscuridad total.

La cámara trabaja con códecs MPEG-4 que ofrecen un consumo de ancho de banda eficiente con compresión de buena calidad y es ideal para la visualización de video en tiempo real; cuenta con códecs MJPEG que ofrece una calidad de video óptima con un método de compresión sin pérdida útil para el almacenamiento masivo hacia un dispositivo de almacenamiento conectado a la red.

Para una información detallada de este producto visite http://www.cisco.com/en/US/docs/security/csbvsc/pvc2300_wvc2300/administration/guide/PVC2300_WVC2300_V20_UG_A.pdf

2.9.4 Teléfono IP Cisco 7960



Fig. 2.13 Teléfono IP Cisco 7960 (Fuente:
http://www.cisco.com/web/ES/solutions/smb/products/voice_conferencing/unified_ip_phones_7900/index.html
ml)

El teléfono IP Cisco 7960 (figura 2.13) es un Teléfono con seis botones programables de línea/característica y cuatro teclas de software que guían al usuario a través de las diferentes características y funciones de las llamadas. Cuenta con una pantalla LCD que muestra la fecha y la hora, el nombre y el número de la persona que realiza la llamada.

Este teléfono permite al usuario ajustar el contraste de la pantalla y seleccionar el tono del timbre y los parámetros de volumen para todo el audio. También es posible establecer preferencias de configuración de la red. La configuración de la red suele definirla el administrador del sistema. La configuración puede definirse de forma automática o manual para DHCP (*Dynamic Host Control Protocol*), TFTP (*Trivial File Transfer Protocol*), CallManager y CallManagers de respaldo.

Este teléfono permite acceder a cualquier información basada en Web utilizando XML para proporcionar un portal a un mundo de características e información en constante crecimiento. Una característica importante de este teléfono es el switch interno Ethernet de dos puertos que permite realizar conexiones directas con redes Ethernet 10/100BaseTx a través de una interfaz RJ-45 con conexión LAN tanto para el teléfono como para un PC en la misma ubicación.

En este diseño de red el administrador del sistema puede designar LAN virtuales independientes (VLAN) (802.1Q) para PCs y teléfonos IP de Cisco.

Para información adicional visite
<http://www.cisco.com/en/US/products/hw/phones/ps379/index.html>

2.9.5 Cisco MCS 7816-I4 Unified Communications Manager Appliance

El Cisco MCS 7816-I4 *Unified Communications Manager Appliance* es un servidor que sirve para unificar las comunicaciones en las redes de datos de una empresa. Ofrece un alto rendimiento, disponibilidad, fácil de instalar y altamente rentable. El dispositivo viene pre instalado con un sistema operativo y el software *Cisco Unified Communications Manager* o también denominado *Cisco Call Manager*.

La aplicación VoIP de este servidor soporta hasta 7500 Teléfonos IP Cisco y 30.000 Teléfono IP Cisco por clúster.

En la tabla 2.8 se muestra los datos técnicos del CISCO MCS 7816-I4

Tabla 2.8 Datos técnicos CISCO MCS 7816-I4

Component	Value
Preload	Cisco Unified Communications Manager 5.1
Processor	Dual Intel 5140 2.33-GHz 4M L2
Memory	4-GB (4 x 1-GB) PC2-5300R
Hard disks	Four 72-GB SAS 2.5-in. hot swap
Remote management	HP iLO Advanced License

2.9.5.1 Cisco Unified Communications Manager

El Cisco *Unified Communications Manager* (CUCM) o *Cisco Call Manager* es un software basado en un sistema de tratamiento de llamadas y telefonía sobre IP desarrollado por Cisco Systems: este software rastrea todos los componentes VoIP activos en la red; esto incluye teléfonos, gateways, puentes para conferencia, recursos para transcodificación, y sistemas de mensajería de voz, entre otros. Este software a menudo utiliza el SCCP (*Skinny*) como un protocolo de comunicaciones para la señalización de parámetros de hardware del sistema como los teléfonos IP. Los protocolos H.323, Media Gateway Control Protocol o SIP son usados para endosar la señalización de las llamadas a los *gateways*.

El *Cisco Unified Communications Manager* es el encargado de evaluar los números llamados y activar los eventos del Gateway para recibir o enviar llamadas a la PSTN. Este software se encuentra instalado en cada MCS (*Media Convergence Server*) o Servidor cisco aprobado. Los MCS se agrupan en un máximo hasta 12 para el procesamiento de llamadas distribuidas y la tolerancia a fallos.

Varios servidores *Cisco Unified CallManager* se agrupan y se administran como una sola entidad en una red IP proporcionando escalabilidad de 1 a 30.000 teléfonos IP por grupo, además de equilibrio de carga y redundancia de servicios de procesamiento de llamadas.

2.9.6 Puntos de acceso inalámbrico de Cisco WAP 2000



Fig. 2.14 AP Cisco WAP 2000 (Fuente: <http://www.cisco.com/en/US/products/ps9945/index.html>)

Los puntos de acceso inalámbrico de Cisco WAP 2000 (figura 2.14) ofrecen una amplia gama de funciones y características, entre las cuales se destacan:

- Capacidad para conectar dispositivos de comunicaciones, tanto cableados como inalámbricos.
- Opciones de conectividad *Wireless-N* (248 Mbps) o *Wireless-G* (54 Mbps), que dependerán del usuario.
- Tecnología *RangeBooster* y MIMO, que aumentan la capacidad de procesamiento inalámbrico y el alcance del router a fin de reducir los "puntos muertos" en el área de cobertura inalámbrica.
- Funciones de seguridad avanzada, que mantienen la red inalámbrica tan segura como la red fija.
- Detección de puntos de acceso dudosos, que explora la red para determinar los intentos de acceso de gateways no autorizados y no seguros a los contenidos protegidos
- Compatibilidad con dispositivos que ofrecen Power over Ethernet, lo que simplifica la instalación y elimina la necesidad y los costos de instalación de fuentes de alimentación externas.
- Instalación y configuración sencillas mediante una interfaz basada en la web

El Cisco WAP2000 combina la tecnología *RangeBooster* con las funciones integradas de calidad de servicio (QoS), Roaming 802.11F y selección automática de canales, por lo que

puede desplegar aplicaciones de VoIP y vídeo de alta calidad en la red. Se puede colocar prácticamente en cualquier sitio mediante un adaptador de corriente estándar o desde un switch *Power-over-Ethernet* o inyector PoE.

El Acces Point AP WAP2000 implementa diferentes tipos de seguridad, entre las cuales se incluye la filtración por MAC y también permite la creación de varias redes inalámbricas (BSSID) que ayudan a crear una red empresarial más segura y una red diferente para dar acceso a los visitantes

La tabla 2.9 muestra las especificaciones Técnicas del AP WAP2000:

Tabla 2.9 Datos técnicos AP WAP2000 (Fuente:
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9692/ps9944/spanish_cisco_pvc2300_business_internet_videocamera.pdf**)**

Transmisión de datos	
Tasa de transferencia (máx)	54 Mbit/s
Wireless LAN features	
Cantidad de canales	13
Antena de refuerzo (max)	3 dBi
Tipo de antena	SMA
Modulación	802.11b/DSSS, 11g/OFDM
Protocolos	
DHCP, cliente	✓
Conectividad	
Tecnología de cableado	10Base-T/100Base-TX
DC-in jack	✓
Ethernet LAN (RJ-45) cantidad de puertos	1
Seguridad	
Algoritmo de seguridad	WEP 64bit/128bit, WPA-PSK, WPA2-PSK, WPA-ENT, WPA2-ENT
Características de la gerencia	
Calidad de servicio (QoS) soporte	✓

Para más información de este equipo visite
http://www.cisco.com/en/US/products/ps5678/Products_Sub_Category_Home.html

2.9.7 Panel de alarma contra incendios VISTA 32FB de HONEYWELL



Fig. 2.15 Panel de alarma VISTA 32FB HONEYWELL (Fuente: <http://www.security.honeywell.com/hsc/products/control/co/14966.html>)

Debido a que cada planta del edificio constará de un panel de alarma con su respectivo comunicador IP se utilizará este panel sencillo con funciones extras que se podrán utilizar para extender el sistema de seguridad en caso de necesitarse, en este caso solo se usa el sistema contra incendios.

El cableado de sistema contra incendios está basado con respecto a la ubicación de los aspersores de agua que tiene el edificio en caso de incendio, todo este sistema de aspersores está ubicado en pasillos del edificio, por lo que los sensores de humo estarán ubicados en los pasillos de habitaciones y otras zonas importantes. Este panel de alarma permite conectar 16 sensores de humo en 2 zonas, en este diseño se usará 1 zona por planta, dejando la otra como reserva en caso de requerir más sensores.

Características principales del panel de alarma contra incendios VISTA 32FB de HONEYWELL

Sistema

- Programación por teclado alfanumérico, software *Downloading*
- Máximo 31 dispositivos periféricos como teclados, módulos de expansión y de relevadores.
- Soporta teclados sensibles al tacto.
- 2 zonas programables de entrada y salida con distintos tiempos.
- 224 eventos en memoria.
- Salida de 2 sirenas de 1.7 A.
- Detección de corte de línea telefónica.
- Corriente auxiliar de 600 mA.

Zonas

- 9 zonas programables, configurables con o sin resistencia de fin de línea.
- Las zonas se pueden configurar de respuesta rápida o lenta.
- Las zonas 1 y 2 soportan hasta 16 detectores de humo en cada una.
- Soporta detectores de humo de 4 hilos.
- Soporta las 23 zonas inalámbricas agregando el receptor **5800** de *Honeywell*.
- Capacidad máxima de 24 Zonas Vplex.
- Soporta módulo de expansión de zonas cableados 4208.
- Supervisión del sistema inalámbrico al 100%.
- Alcance de hasta 60 m en la serie inalámbrica 5800.

Comunicación

- Soporta los formatos de comunicación en 4+2 y *CONTAC/ID*.
- Soporta opción de reporte doble y dividido.
- Compatible con los sistemas de comunicación de tercera generación 3I.

2.9.7.1 Comunicador IP Avatec IPCOM4



Fig. 2.16 IP COM4 (Fuente: <http://www.avatec.com.ar/ipcom.pdf>)

El comunicador IP (figura 2.16) sirve para el envío de información de los eventos generados por el panel de alarma al centro de monitoreo, utilizando para esto la red LAN, Intranet / Internet / GSM / GPRS como su medio de transmisión. Trabaja en dos configuraciones: Ethernet cuando el equipo se conecta a la red (Intranet o Internet) a través de LAN/WAN TCP/IP y GPRS que usa una red GPRS/GSM.

Estos paneles se usan para el envío de todos los eventos generados por el panel de control y solo usa la línea fija como vía alternativa, el denominado estado de *Backup* Telefónico. Para recibir los eventos enviados por el *IPCOM4* es necesario el software *Secure Alert®*

instalado en una PC que será la de administración.

Este equipo mediante el envío de un paquete denominado **“Heart Beat”** cada 60 segundos (o 240 segundos de acuerdo con la programación designada) al centro de monitoreo verifica que la comunicación IP siga vigente, envía 3 paquetes **“Heart Beat”** y si no reciben un ACK (paquete de confirmación) por parte del panel, desconecta la comunicación IP y pasa a operar en el **Modo Backup Telefónico** que utiliza una línea telefónica fija para el envío de eventos.

Cuando el equipo trabaja con conexión IP puede trabajar en **Modo Interceptación y Modo Captura**. En el modo Interceptación el equipo se comunica con una dirección IP (principal) en tanto que en el Modo Captura pueden ser utilizadas dos direcciones IP, siendo una la principal y otra la secundaria. Los protocolos soportados por el *IPCOM4* son: *CONTACT-ID* y 4x2 (en 10 y 20 bps), el equipo se adapta automáticamente a cada uno de los protocolos descritos dependiendo de la cadencia de tonos recibida.

Más información visite la hoja de especificaciones del equipo disponible en <http://www.avatec.com.ar/ipcom.pdf>

CAPÍTULO III

DISEÑO DE LA RED MULTISERVICIO

3.1 Consideraciones para el diseño de red.

Para el diseño de la red multiservicio del presente proyecto se toma en cuenta que la red debe manejar y garantizar la calidad de servicio. Considerando la cantidad de usuarios y aplicaciones que podrán acceder cada uno de ellos se procede a distribuir el tráfico que maneja la red mediante la creación de redes virtuales (VLAN) (*Virtual Local Área Network*), redes que permiten manejar de mejor manera el tráfico y el enrutamiento del mismo reduciendo los problemas de congestión y velocidad.

Las redes VLAN permiten la portabilidad de las estaciones de trabajo en la red LAN, permiten agregar fácilmente estaciones de trabajo a la LAN en cualquiera de las aplicaciones que se necesite demostrando la convergencia de la red. A continuación se explica brevemente que es una red VLAN.

3.2 Redes VLAN.

Una VLAN permite al administrador de red crear grupos de dispositivos conectados de manera lógica que actúen como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN. Cuando se configura una VLAN, puede ser nombrada para describir la función principal de los usuarios de esa VLAN.

En el ejemplo de la figura 3.1 todas las computadoras de los estudiantes se pueden configurar en la VLAN "estudiante". Mediante las VLAN, se puede segmentar de manera lógica las redes conmutadas basadas en equipos de proyectos, funciones o departamentos. También se puede utilizar una VLAN para estructurar geográficamente la red para respaldar la confianza en aumento de las empresas sobre trabajadores domésticos. Estas VLAN permiten que el administrador de la red implemente las políticas de acceso y seguridad para grupos particulares de usuarios. (CISCO)

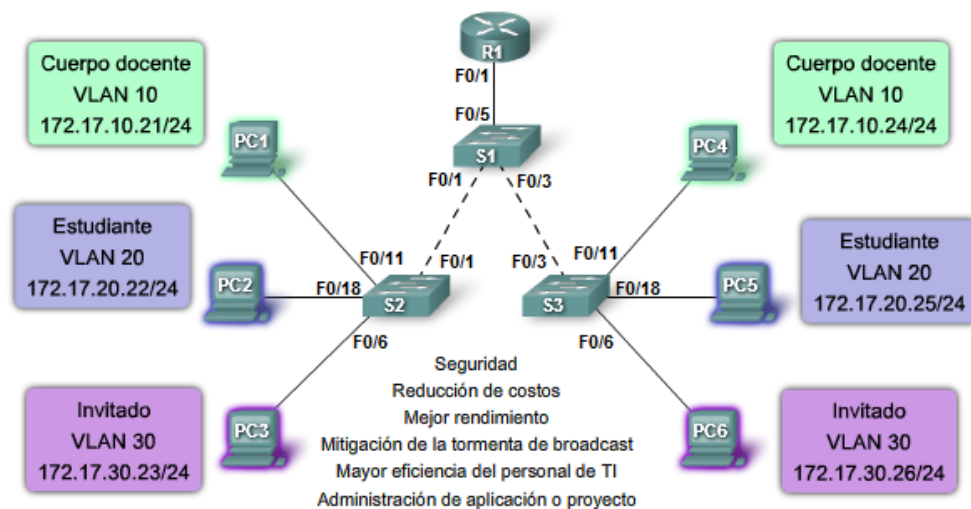


Fig. 3.1 Beneficios de una red VLAN (Fuente: CISCO Modulo CCNA3)

3.2.1 Beneficios de una VLAN

Los principales beneficios al utilizar redes VLAN son los siguientes:

Seguridad: los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.

Reducción de costos: el ahorro en el costo resulta de la poca necesidad de actualizaciones de red caras y usos más eficientes de enlaces y ancho de banda existente.

Mejor rendimiento: la división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.

Mitigación de la tormenta de broadcast: la división de una red en las VLAN reduce el número de dispositivos que pueden participar en una tormenta de broadcast. En la figura 3.1 puede observar que, a pesar de que hay seis computadoras en esta red, hay sólo tres dominios de broadcast: Cuerpo docente, Estudiante e Invitado.

Mayor eficiencia del personal de TI: las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando se proporciona un switch nuevo, todas las políticas y procedimientos que ya se configuraron para la VLAN particular se implementan cuando se asignan los puertos. También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre. En la figura 3.1 para una identificación más fácil se nombró "Estudiante" a la VLAN 20, la VLAN 10 se podría nombrar "Cuerpo docente" y la VLAN 30 "Invitado".

Para el diseño de la red se pretende agrupar a los usuarios de acuerdo con aplicaciones comunes entre ellos, con lo cual el tráfico de la misma se reducirá notablemente.

Los grupos de trabajo de la VLAN estarán constituidos por:

- Red VLAN Almacenes.
- Red VLAN AP.
- Red VLAN Administración.
- Red VLAN Alarmas.
- Red VLAN Voz.
- Red VLAN VideoVigilancia.
- Red VLAN Varios

En las siguientes tablas se muestra especificación de datos en cada planta del edificio

Tabla 3.1 Especificación del sistema de datos de la planta baja

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP
1	Cocina	Dat001				
2	Repostería	Dat002				
3	Despensa	Dat003				
4	Comedor					Dat004
5	Almacén 1		Dat005			
6	Almacén 2		Dat006			
7	Almacén 3		Dat007			
8	Almacén 4		Dat008			
9	Almacén 5		Dat009			
10	Almacén 6		Dat010			
11	Sala de Prensa		Dat011			
12	Sala de Internet			Dat012-Dat016		
13	Sala de reuniones				Dat017	
14	Recepción		Dat018		Dat019	
15	Gerencia		Dat020		Dat021	
16	Contabilidad	Dat022-Dat023			Dat024-Dat025	
17	Secretaría	Dat026	Dat027		Dat028-Dat029	
18	Sala VIP	Dat030				
19	Cafetería	Dat031				Dat032
20	Cocina	Dat031				
21	Habitaciones 1-5	Dat033-Dat037				
22	Habitaciones 6-9	Dat038-Dat041				Dat042
23	Habitaciones 10-13	Dat043-Dat046				
24	Piscina					Dat047-Dat048
25	Sala Entrenadores				Dat049-Dat050	
26	Sala Control				Dat051	
27	Bodega				Dat052	
28	Secado				Dat053	
29	Planchado				Dat054	
30	Recepción	Dat055				
31	Vestíbulo Derecho					Dat056
32	Cámaras	Dat057-Dat070				
33	Panel de Alarma Planta Baja	Dat071				

Tabla 3.1.1 Especificación del sistema de datos de la primera planta

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP
1	Habitaciones 14-17	Dat072-Dat075				
2	Habitaciones 18-21	Dat076-Dat079				Dat080
3	Habitaciones 22-25	Dat081-Dat084				
4	Habitaciones 26-30	Dat085-Dat089				Dat090
5	Habitaciones 31-34	Dat091-Dat094				
6	Habitaciones 35-40	Dat095-Dat100				Dat101
7	Habitaciones 41-44	Dat102-Dat105				
8	Habitaciones 45-49	Dat106-Dat110				Dat111
9	Habitaciones 50-53	Dat112-Dat113				Dat116
10	Habitaciones 54-57	Dat117-Dat120				
11	Habitaciones 58-61	Dat121-Dat124				
12	Cámaras	Dat125-Dat131				
13	Panel de Alarma Primera Planta	Dat132				

Tabla 3.1.2a Especificación del sistema de datos de la segunda planta (a)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP
1	Habitaciones 62-64	Dat133-Dat135				
2	Habitaciones 65-68	Dat136-Dat139				Dat140
3	Habitaciones 69-72	Dat141-Dat144				
4	Habitaciones 73-77	Dat145-Dat149				Dat150
5	Habitaciones VIP 1-2	Dat151-Dat152		Dat153-Dat154		
6	Habitaciones 78-81	Dat155-Dat158				
7	Habitaciones 82-85	Dat159-Dat162				Dat163
8	Habitaciones 86-89	Dat166-Dat167				
9	Cámaras	Dat168-Dat170				
10	Panel de Alarma Segunda Planta (a)	Dat171				

Tabla 3.1.2b Especificación del sistema de datos de la segunda planta (b)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP
1	Habitaciones 90-93	Dat172-Dat175				
2	Habitaciones 94-97	Dat176-Dat179				Dat180
3	Habitaciones 98-100	Dat181-Dat183				
4	Habitaciones VIP 3-4	Dat184-Dat185		Dat186-Dat187		
5	Habitaciones 101-104	Dat188-Dat191				
6	Habitaciones 105-108	Dat192-Dat195				Dat196
7	Habitaciones 109-111	Dat197-Dat199				
8	Cámaras	Dat200-Dat202				
9	Panel Alarma Segunda Planta (b)	Dat203				

Tabla 3.1.3a Especificación del sistema de datos de la tercera planta (a)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP
1	Habitaciones 112-114	Dat204-Dat206				
2	Habitaciones 115-118	Dat207-Dat210				Dat211
3	Habitaciones 119-122	Dat212-Dat215				
4	Habitaciones 123-125	Dat216-Dat218				Dat219
5	Habitaciones VIP 5-6	Dat220-Dat221		Dat222-Dat223		
6	Habitaciones 126-129	Dat224-Dat227				
7	Habitaciones 130-135	Dat228-Dat233				Dat234
8	Cámaras	Dat235-Dat237				
9	Panel Alarma Tercera Planta (a)	Dat238				

Tabla 3.1.3b Especificación del sistema de datos de la tercera planta (b)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP
1	Habitaciones 136-139	Dat239-Dat242				
2	Habitaciones 140-144	Dat243-Dat247				Dat248
3	Habitaciones VIP 7-8	Dat249-Dat250		Dat251-Dat252		
4	Habitaciones 145-148	Dat253-Dat256				
5	Habitaciones 149-153	Dat257-Dat261				Dat262
6	Cámaras	Dat263-Dat265				
7	Panel Alarma Tercera Planta (b)	Dat266				

Tabla 3.1.4a Especificación del sistema de datos de la cuarta y quinta planta (a)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP
1	Oficina extra 1	Dat267			Dat268	
2	Oficina extra 2	Dat269-Dat271			Dat272-Dat274	
3	Oficina extra 3	Dat275			Dat276	
4	Oficina extra 4	Dat277			Dat278-Dat279	
5	Oficina extra 5	Dat280			Dat281-Dat282	
6	Oficina extra 6	Dat283			Dat284-Dat285	
7	Bar extra					
8	Habitaciones VIP 9-10	Dat286-Dat287		Dat288-Dat289		
9	Habitaciones 154-157	Dat290-Dat293				Dat294
10	Habitaciones 158-161	Dat295-Dat298				
QUINTA PLANTA						
1	Habitaciones VIP 13-14	Dat299-Dat300		Dat301-Dat302		
2	Cámaras	Dat303-Dat305				
3	Panel Alarma Cuarta y Quinta Planta (a)	Dat306				

TABLA 3.1.4b Especificación del sistema de datos de la cuarta y quinta planta (b)

ITEM	DESCRIPCIÓN	TELÉFONO IP	TELÉFONO IP + INTERNET	INTERNET 128kbps	RED	AP
1	Habitaciones 162-165	Dat307-Dat310				
2	Habitaciones 166-168	Dat311-Dat313				Dat314
3	Habitaciones VIP 11-12	Dat315-Dat316		Dat317-Dat318		
4	Habitaciones 169-172	Dat319-Dat322				
5	Habitaciones 173-177	Dat323-Dat327				Dat328
QUINTA PLANTA						
1	Habitaciones VIP 15-16	Dat329-Dat330		Dat331-Dat332		
2	Cámaras	Dat333-Dat336				
3	Panel Alarma Cuarta y Quinta Planta (b)	Dat337				

En la tabla 3.1 se tienen 71 puertos de datos que cubren toda la planta baja. Como se puede apreciar en la figura 2.1 de la topología de la planta baja, se cuenta con 2 switches cisco **2960S-48FPS-L**, switches de 48 puertos *fastethernet* con la característica PoE. En la planta baja se tienen 22 puertos de reserva libres para su uso en cualquier momento, en la

tabla 3.1.5 se muestra la distribución de los puertos en cada switch de la planta baja que estarán en el cuarto de telecomunicaciones.

Tabla 3.1.5 Distribución de interfaces de switches de la planta baja

SWITCH (48puertos)	
Interfaz Switch	Descripción
Fa0/1-Fa0/2	Enlaces Troncales
Fa0/3-Fa0/48	Dat001-Dat046
Gi1/1	Enlace Troncal
Gi1/2	Enlace Troncal
Gi1/3	Enlace Troncal
Gi1/3	Enlace Troncal
SWITCH 1(48 puertos)	
Fa0/1	Enlace Troncal
Fa0/2-Fa0/26	Dat047-Dat071
Fa027-Fa0/48	Reservas LAN
Gi1/1	Enlace Troncal
Gi1/2	Enlace Troncal
Gi1/3	Enlace Troncal
Gi1/3	Enlace Troncal

En la primera planta se tienen 61 puertos de datos. La tabla 3.1.6 muestra la distribución de los puertos en las interfaces de los switches que estarán en el cuarto de comunicaciones.

Tabla 3.1.6 Distribución de interfaces de switches de la primera planta

SWITCH 2 (48puertos)	
Interfaz Switch	Descripción
Fa0/1	Enlace Troncal
Fa0/2-Fa0/48	Dat072-Dat118
Gi1/1	Enlace Troncal
Gi1/2	Enlace Troncal
Gi1/3	Enlace Troncal
Gi1/3	Enlace Troncal
SWITCH 3(24 puertos)	
Fa0/1	Enlace Troncal
Fa0/2-Fa0/15	Dat119-Dat132
Fa0/16-Fa0/24	Reservas LAN
Gi1/1	Enlace Troncal
Gi1/2	Enlace Troncal
Gi1/3	Enlace Troncal
Gi1/3	Enlace Troncal

En la segunda planta (a) se tiene 39 puertos de datos. La tabla 3.1.7 muestra la distribución de los puertos en las interfaces de los switches que estarán en el cuarto de comunicaciones.

Tabla 3.1.7 Distribución de interfaces de switches de la segunda planta (a)

SWITCH 4 (48puertos)	
Interfaz Switch	Descripción
Fa0/1-Fa0/39	Dat133-Dat171
Fa0/40-Fa0/48	Reservas LAN
Gi1/1	Enlace Troncal
Gi1/2	Enlace Troncal
Gi1/3	Enlace Troncal
Gi1/3	Enlace Troncal

En la Segunda planta (b) se tiene 32 puertos de datos. La tabla 3.1.8 muestra la distribución de puertos en las interfaces de los switches que estarán en el cuarto de comunicaciones.

Tabla 3.1.8 Distribución de interfaces de switches de la segunda planta (B)

SWITCH 5 (48puertos)	
Interfaz Switch	Descripción
Fa0/1-Fa0/32	Dat172-Dat203
Fa0/33-Fa0/48	Reservas LAN
Gi1/1	Enlace Troncal
Gi1/2	Enlace Troncal
Gi1/3	Enlace Troncal
Gi1/3	Enlace Troncal

En la tercera planta (a) se tiene 35 puertos de datos. La tabla 3.1.9 muestra la distribución de puertos en las interfaces de los switches que estarán en el cuarto de comunicaciones.

Tabla 3.1.9 Distribución de interfaces de switches de la tercera planta (A)

SWITCH 6 (48puertos)	
Interfaz Switch	Descripción
Fa0/1-Fa0/35	Dat204-Dat238
Fa0/36-Fa0/48	Reservas LAN
Gi1/1	Enlace Troncal
Gi1/2	Enlace Troncal
Gi1/3	Enlace Troncal
Gi1/3	Enlace Troncal

En la tercera planta (b) se tiene 35 puertos de datos. La tabla 3.1.10 muestra la distribución de puertos en las interfaces de los switches que estarán en el cuarto de comunicaciones.

Tabla 3.1.10 Distribución de interfaces de switches de la tercera planta (B)

SWITCH 7 (48puertos)	
Interfaz Switch	Descripción
Fa0/1-Fa0/28	Dat239-Dat266
Fa0/36-Fa0/48	Reservas LAN
Gi1/1	Enlace Troncal
Gi1/2	Enlace Troncal
Gi1/3	Enlace Troncal
Gi1/3	Enlace Troncal

Entre la cuarta planta (A) y quinta planta (A) se tiene 40 puertos de datos. La tabla 3.1.11 muestra la distribución de los puertos en las interfaces de los switches que estarán en el cuarto de comunicaciones.

Tabla 3.1.11 Distribución de interfaces de switches de la cuarta y quinta planta (A)

SWITCH 8 (48 puertos)	
Interfaz Switch	Descripción
Fa0/1-Fa0/40	Dat267-Dat306
Fa0/41-Fa0/48	Reservas LAN
Gi1/1	Enlace Troncal
Gi1/2	Enlace Troncal
Gi1/3	Enlace Troncal
Gi1/3	Enlace Troncal

Entre la cuarta planta (B) y quinta planta (B) se tiene 31 puertos de datos. La tabla 3.1.12 muestra la distribución de los puertos en las interfaces de los switches que estarán en el cuarto de comunicaciones.

Tabla 3.1.12 Distribución de interfaces de switches de la cuarta y quinta planta (B)

SWITCH 9 (48 puertos)	
Interfaz Switch	Descripción
Fa0/1-Fa0/31	Dat307-Dat337
Fa0/32-Fa0/48	Reservas LAN
Gi1/1	Enlace Troncal
Gi1/2	Enlace Troncal
Gi1/3	Enlace Troncal
Gi1/3	Enlace Troncal

3.3 Diseño de las redes VLAN

Con el número de switches a usarse y la distribución de los mismos se puede clasificar cada departamento del edificio para la asignación de VLANs. El diseño constará de un total 7 VLANs designadas de la siguiente manera:

- VLAN 10: VLAN Almacenes.
- VLAN 20: VLAN AP.
- VLAN 30: VLAN Administración.
- VLAN 40: VLAN Alarmas.
- VLAN 50: VLAN Voz.
- VLAN 60: VLAN Video Vigilancia.
- VLAN70: VLAN Varios

Toda red VLAN necesita una VLAN de administración, en este diseño se designa la VLAN 99 como VLAN de administración para cada switch.

3.3.1 Asignación de VLANS por Departamentos.

En los anexos 1-7 se muestra la distribución de las 7 redes VLAN en cada Planta del edificio. A pesar de tener varios departamentos en pisos diferentes, mediante la creación de redes VLAN se puede asociar a cada uno de ellos si todos pertenecen a una misma red de servicios en común.

En este diseño se ha reservado algunos puertos de switches y puntos de red a fin de solventar la escalabilidad del edificio a futuro, estos puertos y puntos de red no pertenecen a ninguna VLAN, estarán conectados físicamente pero sus puertos en los switches estarán desactivados para no consumir energía innecesaria por parte del switch, el momento que se requiera el uso de estos puertos, el administrador de red tendrá que levantar la interfaz del switch y asignarle a tal puerto una VLAN para iniciar su funcionamiento.

3.4 Funcionamiento y configuración de los equipos de red.

A continuación se explica brevemente el funcionamiento de los equipos de red y la configuración básica de los mismos: Todos los puntos de red irán a su TC correspondiente en cada piso, cada TC contará con un rack de comunicaciones con los switches a utilizarse en cada planta, cada punto de red pasará por un *patch panel* para la organización de cables en el rack de comunicaciones, cada switch estará conectado en cascada con el otro mediante los puertos reservados como enlaces troncales (Puertos *Gigabit Ethernet*).

Para el *backbone* de datos se escoge fibra multimodo para aprovechar los beneficios de la fibra óptica y los interfaces de fibra que tiene cada switch en sus enlaces troncales de tipo *Gigabit Ethernet*.

Todos los switches estarán comunicados hasta el switch principal que se conectará al router. El router es el encargado de la comunicación de todas las VLAN en caso de requerir que ciertos departamentos tengan comunicación con otros departamentos de una VLAN diferente. El presente proyecto explica la creación de una red multiservicio básica para el edificio que se refiere. A continuación se detallan las configuraciones básicas para el router y switches utilizados para garantizar la conectividad de todos los puntos de red.

El router CISCO 2800 funciona como *gateway* para los servicios de telefonía IP, es decir, mediante el software *Cisco Call Manager* podrá conmutar las llamadas IP con la red de telefonía pública PSTN. El *Cisco Call manager* es un software pre instalado en el servidor **Cisco MCS 7816-I4 Unified Communications Manager** resultando ser un servidor de antivirus o un active directory, este necesariamente va conectado al router o a un switch en una VLAN de servidores y conectado a la interfaz del router. Esta conectividad permite al servidor salir, ver la red y viceversa.

Para telefonía IP se tiene 3 tipos de llamadas: internas, locales y a celulares; para llamadas internas es necesario que el software *Cisco Call Manager* sea configurado desde el MCS 7816-I4 en todos sus parámetros: región, SRST, *partition*, *gateway*, *route list*, *route group*, *calling searching space*, troncales, *cti route point*, las direcciones MAC de los teléfonos que se van a conectar con su respectiva extensión y la configuración del Proxy SIP para la comunicación entre los dispositivos SIP. Para acceder a la interfaz de configuración se ingresa la IP nativa del dispositivo y se puede configurar cada parámetro según los requerimientos de la empresa.

La configuración del *Cisco Call Manager* para direccionar llamadas internas, locales y a celulares se realiza de la siguiente manera: para llamadas a convencional ETAPA deja una línea telefónica o varias líneas telefónicas en el edificio, las mismas que deben ser conectadas a un *gateway* de voz, en este caso el router CISCO 2800 que tiene capacidad para albergar interfaces FXO para telefonía, cada una de las interfaces deben ser configuradas en el *Cisco Call Manager* para su uso en llamadas locales, celulares o internas. Para llamadas a celular el procedimiento es igual al de llamadas convencionales, con la diferencia que se utilizan bases celulares que deja el operador de telefonía celular, la conexión es con un cable telefónico de la base a la interfaz FXO.

En el router donde se configuran los interfaces FXO, se debe constar en el *running config* el *hostname* del servidor call manager con el comando:

- ccm-manager config server [ip_del _servidor_call_manager_]
- ccm-manager config

Estos comandos informan al router que adopte la configuración del servidor *call manager* y que asigne a cada interfaz FXO la responsabilidad de conmutar la telefonía Local, Celular o interna.

Al usar en el router el comando ***telephony-service setup*** se inicia el proceso de configuración de todo el sistema de telefonía IP: lenguaje del sistema, número de teléfonos a usarse, número de líneas y de interfaces FXO, activación del protocolo *skinny* (Protocolo de Cisco para teléfonos IP para determinar los puertos a usar (puerto TCP 2000)), tono de marcado, asignación de números para cada teléfono.

Para el sistema de VideoVigilancia cada cámara estará dentro de su red VLAN y desde los computadores principales en el cuarto de telecomunicaciones se podrá tener acceso a cada una de ellas para el monitoreo en tiempo real de todo el sistema del edificio. Cada cámara IP puede ser configurada para enviar sus datos a una IP remota que puede ser alguna PC conectada a un servidor de video o NVR (*network video recorder*).

Tabla 3.2. Tabla de Calidad y ancho de banda Cámara PVC2300

Resolution	Quality	Frame Rate	Bandwidth (k/bps)	
			MPEG-4	MJPEG
640 x 480	Very High	30	2320	3040
		15	1840	2800
		6	880	1840
	Normal	30	2240	2800
		15	1680	2640
		6	640	1600
	Very Low	30	2160	2640
		15	1200	2400
		6	560	1200

La cámara escogida para este diseño fue la cámara IP Cisco PVC2300, una cámara que comprime video usando diferentes códecs, entre ellos el codec MPEG-4, que tiene compresión con *Bitrate* variable. Se usa la resolución de video de alta calidad de la cámara que en el caso más crítico, es decir, trabajando a su máxima capacidad consumirá un ancho de banda de 2320 Kbps, que por un total de 40 cámaras da cerca de 92Mbps para ser administrados desde el computador central, estas condiciones son extremas y puede que nunca se den debido que las cámaras consumen mucho menos y diferente ancho de banda. La administración de la VLAN de Videovigilancia podrá hacerse sin inconvenientes.

Para el sistema de alarma contra incendios se usa un dispositivo de hardware denominado comunicador IP, el cual trabaja en modo de intercepción y en modo de backup telefónico, en modo intercepción el IPCOM simula una línea hacia el panel que provee todas las tensiones y señales necesarios para que el panel de alarma “piense” que está conectado a una línea telefónica fija. El IPCOM captura la información y la envía por Internet, en este caso a la red VLAN de Videovigilancia que reportará los eventos a un computador central. En este modo, la línea telefónica fija queda sin uso.

Cuando está funcionando en el modo de Backup Telefónico, el usuario se conecta al panel y el panel se conecta a la línea de telefonía pública, quedando el IPCOM fuera del circuito lo que significa que los eventos dejan de ser enviados a la red VLAN de Videovigilancia y son transmitidos hacia una línea telefónica que puede ser de emergencia.

El protocolo de comunicación que usará el comunicador IP será el protocolo *CONTACT ID*, protocolo que el panel de alarma usa en este diseño de red.

En la tabla 3.3 se muestra los bits de programación para la configuración de este equipo.

Tabla 3.3 Servicios Disponibles Comunicador IP de Avatec. (Tabla tomada de [www.avatec.com](http://www.avatec.com.ar/comunicador_ip02.htm))

Bit 0	Servicio 1	Si está activado cambia el tiempo entre envío de paquetes de HEART BEAT a 240 segundos. Si no el tiempo entre HEART BEAT's es de 60 segundos (default activado)
Bit 1	Servicio 2	Si está activado cambia el tiempo interdígitos a 6 segundos. Desactivado es de 2 segundos (default desactivado)
Bit 2	Servicio 3	No utilizado
Bit 3	Servicio 4	Si está activado hace que el COMUNICADOR IP pase a modo de BACKUP Telefónico cuando no entiende el protocolo de comunicación del panel de alarmas (default activo)
Bit 4	Servicio 5	No utilizado
Bit 5	Servicio 6	No utilizado
Bit 6	Servicio 7	No utilizado
Bit 7	Servicio 8	Reduce a la mitad todos los tiempos del IP COM (default desactivado)

Para configurar estos servicios del comunicador IP es necesario ingresar el modo de programación. Cada comunicador IP cuenta con una dirección IP a la cual el administrador de red puede acceder desde una computadora central que estará ubicada en el cuarto principal de telecomunicaciones.

La configuración de APs es muy similar a la configuración de un router inalámbrico casero que se tiene comúnmente en los hogares, ingresando a su IP default se puede asignar un direccionamiento DHCP para la asignación de direcciones IP de manera dinámica para los equipos que se conecten a estos, además de poder configurar seguridades de la red, filtración MAC, ocultar la red en caso de poseer redes privadas, etc.

El router es el encargado del enrutamiento de todas las redes, es el puente de paso entre cada dispositivo de red y su servidor, puede implementar calidad de servicio y prioridades para aplicaciones que requieran más importancia en el funcionamiento pleno de la red.

La configuración de los switches resulta ser una parte fundamental de la red, son los encargados de segmentar lógicamente la red principal. Se cuenta con 10 switches en total que están repartidos por todo el edificio, la manera más útil de configurar estos equipos es usar el protocolo VTP (*Vlan Trunking Protocol*), protocolo que permite la configuración de VLAN y administración de las mismas, este protocolo permite repartir la información a otros switches sobre las VLAN creadas en la red. Este protocolo puede ser configurado en tres modos: servidor, cliente y modo transparente.

Se configura al Switch 1 como servidor, dentro de este se configuran las VLAN. La configuración se la hace desde la línea de comandos del dispositivo y es la siguiente:

- **Switch1(config) # vtp mode server** (Este comando hace al Switch 1 servidor)
- **Switch1(config) # vtp domain CAR** (Este comando establece el nombre de dominio VTP para toda la red, es muy importante q en cada switch se establezca el mismo nombre de dominio para que la distribución de VLANs por parte del switch servidor llegue a todos los switches de la red.)
- **Switch1(config) # vtp password xxxxxxxx** (Este comando establece una contraseña de administración)

Para la creación de las VLANs en el servidor la configuración es la siguiente:

- **Switch(config) # vlan 99**
- **Switch(config-vlan) # name management**
- **Switch(config-vlan) #exit**

Este comando asigna la vlan 99 como vlan de administración de switches. Se sigue el mismo procedimiento para configurar las VLAN de toda la red.

Al realizar este proceso de configuración del switch servidor VTP, este guardará todas las VLAN que se han configurado. La configuración en el resto de switches es la siguiente:

- **Switch1(config) # vtp mode client** (Este comando hace al Switch 2 cliente)
- **Switch1(config) # vtp domain CAR** (Como se menciona anteriormente todos los switches deben tener el mismo nombre de dominio VTP)
- **Switch1(config) # vtp password xxxxxxxx** (Este comando establece una contraseña de administración)

Al configurar los switches 1 hasta el 9 en modo cliente, recibirán mediante el switch servidor la información de las VLAN de la red, así al conectar un nuevo switch este recibirá la información de las VLANs existentes. Al realizar esta configuración se debe asignar cada puerto de los switches a la VLAN que pertenecen. Las tablas de distribución de puertos de switches presentadas en los anexos 1-7 muestran la configuración de VLANs para los puertos de cada switch. Al realizar este proceso se pondrá a toda la red en funcionamiento, todas las máquinas podrán hacer ping en su red VLAN lo cual demuestra la comunicación de los equipos.

La configuración del router para el manejo de VLANs y enrutamiento de paquetes entre VLANs es la siguiente: se crean subinterfaces dentro de la interfaz Fa0/0 del router asignando la encapsulación seguida del número de la VLAN, la primera VLAN es la nativa por *default* aunque se puede cambiar a otra.

Comandos para la configuración del router y DHCP

- R1(config)#interface FastEthernet0/0.1
- R1(config-if)#encapsulation dot1Q 99 native
- R1 (config-subif)# ip address 192.168.10.1 255.255.255.0
- R1(config)#interface FastEthernet0/0.10
- R1(config-if)#encapsulation dot1Q 10
- R1 (config-subif)# ip address 192.168.11.1 255.255.255.0
- R1(config)#interface FastEthernet0/0.20
- R1(config-if)#encapsulation dot1Q 20
- R1(config-subif)#ip address 192.168.12.1 255.255.255.0

Los comandos presentados asignan a la interfaz *fastethernet0/0* del router como interfaz de comunicación para las VLANs. Un router no cuenta con varias interfaces *fastethernet* por lo que se procede a subdividir la interfaz para asignar a cada VLAN una subinterfaz por la cual se hará el enrutamiento de paquetes. El ejemplo de comandos presentado presenta configuraciones para la VLAN nativa, la vlan de Almacenes y la Vlan de AP, la configuración

para el resto de VLANs es la misma con la diferencia que se debe asignar una dirección IP diferente para cada Vlan.

Después se crean las IP de exclusión y los pool

- ip dhcp excluded-address **192.168.10.1 192.168.10.10**
- ip dhcp excluded-address 192.168.11.1 192.168.11.10
- ip dhcp excluded-address 192.168.12.1 192.168.12.10
- ip dhcp pool **vlan10**
- Network 192.168.10.0 255.255.255.0
- Default-router 192.168.10.1
- ip dhcp pool **vlan20**
- Network 192.168.11.0 255.255.255.0
- Default-router 192.168.11.1
- ip dhcp pool **vlan30**
- Network 192.168.12.0 255.255.255.0
- Default-router 192.168.12.1

Esta configuración determina un rango de direcciones IP para que se proporcionen mediante DHCP, el procedimiento es igual hasta la VLAN 70. Al configurar los switches en modo VTP tendrán las VLANs asignadas, resta asignar las PCs a cada switch cliente y que el IP se proporcione mediante DHCP.

Esta configuración básica de la red multiservicio del CENTRO DE ALTO RENDIMIENTO DE “TOTORACocha” brindara conectividad entre cada dispositivo de red que pertenezca a una misma VLAN, segmentando tráfico y dando prioridades según lo desee el administrador de red. Las prioridades a implementarse pueden seguir el siguiente orden: Telefonía IP- Videovigilancia-Datos o puede variar según las necesidades del edificio. Todas estas configuraciones pueden ser realizadas desde el router usando la línea de comandos de cada dispositivo CISCO.

3.5 Costo de equipos a implementarse en el diseño de red.

El presente diseño abarca un costo estimado de los equipos principales que forman la red. La tabla 3.4 muestra el costo aproximado de los EQUIPOS que se utilizarán en el diseño de red, la tabla no incluye metros de cable a utilizarse, precios de *patch cords*, ni de terminales *Ethernet*.

Tabla 3.4 Costos de equipos de red para la implementación del diseño de red.

DESCRIPCIÓN	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
Router Cisco serie 2800	1	4200	4200
Switch Cisco serie 2960 con Poe (48 puertos)	9	3352	30168
Switch Cisco serie 2960 con Poe (24 puertos)	1	1785	1785
Cisco MCS 7816-I4	1	3416.57	3416.57
Cámara IP Cisco PVC2300	40	378	15120
Teléfono IP Cisco 7960	220	121	26620
AP Cisco WAP 2000	24	150	6000
Panel de Alarma Honeywell vista32BP con comunicador IP	8	350	2800
Sensores de humo	85	38	3230
TOTAL			93339.57

El costo de los equipos a utilizarse en el diseño de red será aproximadamente de 92339.57 \$

CONCLUSIONES

Con el presente trabajo monográfico se concluye que para brindar servicios buena calidad a los usuarios de una empresa, es necesaria la implementación de una red multiservicio basada en protocolo IP que facilite notablemente la administración de servicios y comodidades para el usuario.

El diseño de red propuesto está en capacidad de brindar servicios de video, voz y datos en una misma plataforma de red con equipos de alta tecnología, además de integrar a la red un sistema de alarma contra incendios inteligente, lo que demuestra las ventajas del protocolo IP para la administración de estos sistemas en una misma infraestructura.

Las redes clásicas de telefonía necesitan centralillas para las comunicaciones internas con un número limitado de teléfonos a conectarse, estos esquemas demuestran mucha vulnerabilidad a las interferencias y representan altos costos de operación; el presente diseño muestra una solución a este tipo de problemas mediante la implementación del *Cisco Call Manager*, una alternativa para el procesamiento de llamadas IP sumamente rentable, de alta disponibilidad y que permite escalabilidad de 1 a 30000 teléfonos IP por grupo, además de poder implementar políticas de calidad de servicio QoS con bajos costos de operación.

El consumo de energía de estos dispositivos es bajo gracias a la característica PoE que permite alimentar directamente cada dispositivo de red desde los switches. Para el caso de video vigilancia, este diseño muestra una gran ventaja que permite la ubicación de las cámaras en cualquier lugar que se desee sin tener en cuenta una toma eléctrica para la alimentación de las mismas, además de poder hacer uso de cámaras de alta definición si la vigilancia del edificio lo necesitase.

La implementación de este tipo de redes llega a ser de fácil administración gracias al uso de redes VLAN que contribuyen de manera significativa a simplificar el tráfico de la misma, segmentando de manera lógica varias subredes sin importar la ubicación de cada usuario y pueden ser controladas por un administrador de red desde un solo cuarto principal de telecomunicaciones.

El diseño presentado deja abierta la posibilidad de implementar nuevos servicios, debido a que los equipos CISCO planteados cuentan con varias características ventajosas para nuevas prestaciones multimedia.

RECOMENDACIONES

Para aprovechar mejor el ancho de banda y la eficacia de todos los equipos de red en la transmisión de voz y video se recomienda escoger los códecs adecuados que permitan realizar una buena compresión, consuman un mínimo de recursos en los cables de red pero que brinden una buena calidad permitiendo la optimización la red.

Es importante adecuar de manera correcta los cuartos de telecomunicaciones y tener por lo menos uno por cada planta para poder distribuir de mejor manera los puntos de red y realizar una correcta organización de los cables UTP en cada *patch panel*, además de tomar en cuenta las normas para el cableado estructurado, entre las más significativas, el no exceder los 100 metros de cableado horizontal y usar escalerillas metálicas para la distribución del mismo y poder facilitar el mantenimiento y la localización de todos los puntos de red.

Se recomienda realizar un enlace redundante de cableado vertical o de *backbone* para solventar posibles fallos en el cableado de *backbone* principal, además de etiquetar cada cable y punto de red en los *patch panels* y en los puertos de los switches para así poder ubicar de manera más fácil para dispositivo que conforma la red.

En el sistema de alarma contra incendios se recomienda ubicar los paneles de alarma en sectores donde solo el administrador de red tenga acceso y no exceder los 10 mts de longitud entre el panel de alarma y el comunicador IP. Se pueden colocar pulsantes de emergencia que serán los encargados de dar la señal de alarma manualmente. Se pueden implementar hasta 4 por planta.

Finalmente se exhorta implementar prioridades, seguridades y políticas de calidad de servicio en cada switch y router para mejorar la estabilidad de la red, además de considerar que la misma debe ser administrada por personal altamente calificado para que no sufra deterioros por su mal uso.

BIBLIOGRAFÍA

REFERENCIAS BIBLIOGRÁFICAS

- ASTERISK CURSO VOZ SOBRE IP Y ASTERISK v1.0. Módulo I. Documento PDF. Diseño de sistemas básicos sobre Voz sobre IP, codecs y protocolos. [consulta 28 de abril 2011].
- CISCO CCNA3: LAN Switching and Wireless Version 4.0 Spanish. Documento PDF. Descripción, funcionamiento, y configuración y enrutamiento de VLANs en redes locales. [consulta 5 de mayo 2011].
- UIT-T Rec. UIT-T Y.2001 (12/2004). Documento PDF. Normas y Recomendaciones sobre redes NGN de la Unión Internacional de Telecomunicaciones. [consulta 30 de abril 2011].
- URIBE, Diego. Módulo de Redes de Nueva Generación (Enero 2011). Funcionamiento, características de sistemas NGN y aplicaciones. [consulta 5 de mayo de 2011].

REFERENCIAS ELECTRÓNICAS

- AVATEC. «Comunicador IP AVATEC» Características, configuración y funcionamiento del comunicador IP AVATEC. Disponible en <http://www.avatec.com.ar/ipcom.pdf> [consulta 2 de junio de 2011].
- AXIS. «Tipos de cámaras IP» Tipos y características principales de cámaras IP. Disponible en http://www.axis.com/es/products/video/camera/about_cameras/types.htm [consulta 20 de Junio de 2011].
- CHERZANAS, Luciano, DOBLADEZ, Maximiliano. «Ancho de Banda por Cliente» Métodos usados para el cálculo de ancho de banda estimado de internet. Disponible en <http://under-linux.org/f105/calculando-largura-de-banda-por-cliente-118846/> [consulta 1 de Julio 2011].
- CISCO. «Voz sobre IP» Equipos CISCO para usarse en diseño de sistemas de telefonía IP Disponible en www.cisco.com/web/ES/solutions/es/voice_over_ip/ [consulta 13 de Julio de 2011].
- DLINK. «VideoVigilancia IP» Conceptos principales y funcionamiento de sistemas de Videovigilancia. Disponible en http://www.dlink.es/cs/Satellite?c=Guide_P&childpagename=DLinkEurope-ES/DLGeneric&cid=1197380409000&p=1197318960420&packedargs=locale=1195806681347&pagename=DLinkEurope-ES/DLWrapper [consulta 25 de Julio de 2011].

- ENCUESTRA PRECIOS. «Precios Switches CISCO» Costos aproximados de Equipos y dispositivos de red CISCO. Disponible en <http://www.encuentraprecios.es/categoria.aspx?id=131&libera=cisco+catalyst+2960&page=2&sort=Prezzo&sortdir=0> [consulta 12 de agosto de 2011].
- EPN. «Sistemas de VideoVigilancia». Tipos de sistemas de Videovigilancia y características principales. Disponible en <http://biblioteca.epn.edu.ec/catalogo/fulltext/CD-1239.pdf> [consulta 15 de agosto de 2011].
- MORA, Luis René «Telefonía IP» Funcionamiento de sistemas de telefonía IP y elementos implicados. Disponible en <http://lrmora.blogspot.com/2008/04/telefonip.html> [consulta 7 de agosto de 2011].
- NETWORK WORLD «Hacia las Redes Multiservicio» Conceptos principales y antecedentes. Disponible en http://www.networkworld.es/Hacia-las-redes-multiservicio_Requerimientos-y-opciones/seccion/articulo-119864 [consulta 3 de mayo de 2011].
- NEXTAG. «Honeywell Productos». Costos estimados de sistemas de alarma contra incendios. Disponible en <http://www.nextag.com/honeywell-ademco-vista-20p/stores.html> [consulta 8 de agosto de 2011]
- NWS «Sistemas de Alarma contra incendio» Tipos y características de los sistemas de alarma contra incendios. Disponible en www.nws.pe/alarmaincendio2.pdf [consulta 8 de Julio de 2011].
- SECURITY ARTWORK. «Funcionamiento Protocolo SIP» Tipos de Protocolos para Voz sobre IP y funcionamiento de protocolo SIP. Disponible en <http://www.securityartwork.es/2008/03/03/voip-protocolo-sip/> [consulta 23 de Junio de 2011].
- SILENT KNIGHT. «honeywell systems». Características de equipos que se usan en seguridad contra incendios. Disponible en <http://www.silentknight.com/index.htm> [consulta 30 de Abril de 2011].

ANEXOS

ANEXO 1: DISTRIBUCIÓN VLAN 10: ALMACENES

ITEM	DESCRIPCIÓN	DATOS
PLANTA BAJA		
5	Almacén 1	Dat005
6	Almacén 2	Dat006
7	Almacén 3	Dat007
8	Almacén 4	Dat008
9	Almacén 5	Dat009
10	Almacén 6	Dat010

ANEXO 2: DISTRIBUCIÓN VLAN 20: VLAN AP

ITEM	DESCRIPCIÓN	DATOS
PLANTA BAJA		
4	Comedor	Dat004
19	Cafetería	Dat032
22	Habitaciones 6-9	Dat042
24	Piscina	Dat047- Dat048
31	Vestíbulo Derecho	Dat056
PRIMERA PLANTA		
2	Habitaciones 18-21	Dat080
4	Habitaciones 26-30	Dat090
6	Habitaciones 35-40	Dat101
8	Habitaciones 45-49	Dat111
9	Habitaciones 50-53	Dat116
SEGUNDA PLANTA (a)		
2	Habitaciones 65-68	Dat140
4	Habitaciones 73-77	Dat150
7	Habitaciones 82-85	Dat163
SEGUNDA PLANTA (b)		
2	Habitaciones 94-97	Dat180
6	Habitaciones 105-108	Dat196
TERCERA PLANTA (a)		
2	Habitaciones 115-118	Dat211
4	Habitaciones 123-125	Dat219
7	Habitaciones 130-135	Dat234

TERCERA PLANTA (b)		
2	Habitaciones 140-144	Dat248
5	Habitaciones 149-153	Dat262
CUARTA Y QUINTA PLANTA (a)		
9	Habitaciones 154-157	Dat294
2	Habitaciones 166-168	Dat314
CUARTA Y QUINTA PLANTA (b)		
5	Habitaciones 173-177	Dat328

ANEXO 3: DISTRIBUCIÓN VLAN 30: VLAN Administración

ITEM	DESCRIPCIÓN	DATOS	LAN
PLANTA BAJA			
13	Sala de reuniones		Dat017
14	Recepción	Dat018	Dat019
15	Gerencia	Dat020	Dat021
16	Contabilidad		Dat024-Dat025
17	Secretaria	Dat027	Dat028-Dat029
18	Sala VIP		

ANEXO 4: DISTRIBUCIÓN VLAN 40: VLAN Alarmas.

ITEM	DESCRIPCIÓN	DATOS
33	Panel de alarma Planta Baja	Dat071
13	Panel de Alarma Primera Planta	Dat132
10	Panel de Alarma Segunda Planta (a)	Dat171
9	Panel Alarma Segunda Planta (b)	Dat203
9	Panel Alarma Tercera Planta (a)	Dat238
7	Panel Alarma Tercera Planta (b)	Dat266
3	Panel Alarma Cuarta y Quinta Planta (a)	Dat306
3	Panel Alarma Cuarta y Quinta Planta (a)	Dat337

ANEXO 5: DISTRIBUCIÓN VLAN50: VLAN Voz

ITEM	DESCRIPCIÓN	DATOS	DATOS
PLANTA BAJA			
1	Cocina	Dat001	
2	Repostería	Dat002	
3	Despensa	Dat003	
5	Almacén 1		Dat005
6	Almacén 2		Dat006
7	Almacén 3		Dat007
8	Almacén 4		Dat008
9	Almacén 5		Dat009
10	Almacén 6		Dat010
11	Sala de Prensa		Dat011
14	Recepción		Dat018
15	Gerencia		Dat020
16	Contabilidad	Dat022-Dat023	
17	Secretaria	Dat026	Dat027
18	Sala VIP	Dat030	
19	Cafetería	Dat031	
20	Cocina	Dat031	
21	Habitaciones 1-5	Dat033-Dat037	
22	Habitaciones 6-9	Dat038-Dat041	
23	Habitaciones 10-13	Dat043-Dat046	
30	Recepción Lavado	Dat055	
PRIMERA PLANTA			
1	Habitaciones 14-17	Dat072-Dat075	
2	Habitaciones 18-21	Dat076-Dat079	
3	Habitaciones 22-25	Dat081-Dat084	
4	Habitaciones 26-30	Dat085-Dat089	
5	Habitaciones 31-34	Dat091-Dat094	
6	Habitaciones 35-40	Dat095-Dat100	
7	Habitaciones 41-44	Dat102-Dat105	
8	Habitaciones 45-49	Dat106-Dat110	
9	Habitaciones 50-53	Dat112-Dat113	
10	Habitaciones 54-57	Dat117-Dat120	
11	Habitaciones 58-61	Dat121-Dat124	
SEGUNDA PLANTA (a)			
1	Habitaciones 62-64	Dat133-Dat135	
2	Habitaciones 65-68	Dat136-Dat139	
3	Habitaciones 69-72	Dat141-Dat144	
4	Habitaciones 73-77	Dat145-Dat149	
5	Habitaciones VIP 1-2	Dat151-Dat152	
6	Habitaciones 78-81	Dat155-Dat158	
7	Habitaciones 82-85	Dat159-Dat162	
8	Habitaciones 86-89	Dat166-Dat167	
SEGUNDA PLANTA (b)			
1	Habitaciones 90-93	Dat172-Dat175	
2	Habitaciones 94-97	Dat176-Dat179	

3	Habitaciones 98-100	Dat181-Dat183	
4	Habitaciones VIP 3-4	Dat184-Dat185	
5	Habitaciones 101-104	Dat188-Dat191	
6	Habitaciones 105-108	Dat192-Dat195	
7	Habitaciones 109-111	Dat197-Dat199	
TERCERA PLANTA (a)			
1	Habitaciones 112-114	Dat204-Dat206	
2	Habitaciones 115-118	Dat207-Dat210	
3	Habitaciones 119-122	Dat212-Dat215	
4	Habitaciones 123-125	Dat216-Dat218	
5	Habitaciones VIP 5-6	Dat220-Dat221	
6	Habitaciones 126-129	Dat224-Dat227	
7	Habitaciones 130-135	Dat228-Dat233	
TERCERA PLANTA (b)			
1	Habitaciones 136-139	Dat239-Dat242	
2	Habitaciones 140-144	Dat243-Dat247	
3	Habitaciones VIP 7-8	Dat249-Dat250	
4	Habitaciones 145-148	Dat253-Dat256	
5	Habitaciones 149-153	Dat257-Dat261	
CUARTA Y QUINTA PLANTA (a)			
1	Oficina extra 1	Dat267	
2	Oficina extra 2	Dat269-Dat271	
3	Oficina extra 3	Dat275	
4	Oficina extra 4	Dat277	
5	Oficina extra 5	Dat280	
6	Oficina extra 6	Dat283	
8	Habitaciones VIP 9-10	Dat286-Dat287	
9	Habitaciones 154-157	Dat290-Dat293	
10	Habitaciones 158-161	Dat295-Dat298	
1	Habitaciones VIP 13-14	Dat299-Dat300	
CUARTA Y QUINTA PLANTA (b)			
1	Habitaciones 162-165	Dat307-Da310	
2	Habitaciones 166-168	Dat311-Dat313	
3	Habitaciones VIP 11-12	Dat315-Dat316	
4	Habitaciones 169-172	Dat319-Dat322	
5	Habitaciones 173-177	Dat323-Dat327	
1	Habitaciones VIP 15-16	Dat329-Dat330	

ANEXO 6: DISTRIBUCIÓN VLAN 60: VLAN Video Vigilancia

ITEM	DESCRIPCIÓN	DATOS
PLANTA BAJA		
32	Cámaras	Dat057-Dat070
PRIMERA PLANTA		
12	Cámaras	Dat125-Dat131
SEGUNDA PLANTA (a)		
9	Cámaras	Dat168-Dat170
SEGUNDA PLANTA (b)		

8	Cámaras	Dat200-Dat202
TERCERA PLANTA (a)		
8	Cámaras	Dat235-Dat237
TERCERA PLANTA (b)		
6	Cámaras	Dat263-Dat265
CUARTA Y QUINTA PLANTA (a)		
2	Cámaras	Dat303-Dat305
CUARTA Y QUINTA PLANTA (b)		
2	Cámaras	Dat333-Dat336

ANEXO 7: DISTRIBUCIÓN VLAN70: VLAN Varios

PLANTA BAJA		
12	Sala de Internet	Dat012-Dat016
SEGUNDA PLANTA (a)		
5	Habitaciones VIP 1-2	Dat153-Dat154
SEGUNDA PLANTA (b)		
4	Habitaciones VIP 3-4	Dat186-Dat187
TERCERA PLANTA (a)		
5	Habitaciones VIP 5-6	Dat222-Dat223
TERCERA PLANTA (b)		
3	Habitaciones VIP 7-8	Dat251-Dat252
CUARTA Y QUINTA PLANTA (a)		
8	Habitaciones VIP 9-10	Dat288-Dat289
1	Habitaciones VIP 13-14	Dat301-Dat302
CUARTA Y QUINTA PLANTA (b)		
3	Habitaciones VIP 11-12	Dat317-Dat318
1	Habitaciones VIP 15-16	Dat331-Dat332

ANEXO 8: [Diseño de la red multiservicio de la planta baja](#)

ANEXO 9: [Diseño de la red multiservicio de la primera planta](#)

ANEXO 10: [Diseño de la red multiservicio de la segunda planta](#)

ANEXO 11: [Diseño de la red multiservicio de la tercera planta](#)

ANEXO 12: [Diseño de la red multiservicio de la cuarta planta](#)

ANEXO 13: [Diseño de la red multiservicio de la quinta planta](#)

ANEXO 14: [Diagrama vertical de la red multiservicio](#)